Harvard Model Congress
Boston 2022

CYBERSECURITY AND DEFENDING CRITICAL INFRASTRUCTURE

By Lap Nguyen

Long Gas lines in Charlotte N.C. after the Colonial Pipeline ransomware attack
NY Times

INTRODUCTION

On May 7th, 2021, Colonial Pipeline Inc. found itself in hot water as ransomware had taken over the operating system and shut down fuel access to 45% of the East Coast (Eaton, 2021). What ensued was a scene straight from a bygone era, the 1970s, as gas shortages gripped the region leading to rationing, long gas lines, and disruption to supply chains. The paralysis of an entire region's economic engine, albeit briefly, highlights the vulnerability of the United States when it comes to defending critical infrastructure in cyberspace.

The maintenance of critical United States infrastructure is performed primarily by the private sector with added oversight by the government. Although this system has worked in the past, the rapid rise of **cybersecurity** threats has highlighted the strong urgency for reform. The President's National Infrastructure Advisory Council (NIAC) highlighted four key factors that inhibit the effectiveness of the current federal capabilities for cyber defense: (1) Private Sector knowledge of federal capabilities is limited, (2) Legal and administrative constraints hinder access to knowledge, (3) Government capabilities are scattered making navigation and coordination difficult, and (4) Classification of essential threat information can delay response (NIAC, 2017).

Cybersecurity *– The protection of internet-connected system from threats online. This may include hardware, software, and data.*

The Council of Economic Advisors estimated that the economic loss from cybercrime in the United States is around $57-109 billion in 2016 with an expectation that it has risen since then (CEA, 2018). The increasing threats from cyberattacks from foreign adversaries, primarily Russia, on critical government systems as well as the private sector necessitate Congress to take action to defend America's cyberspace. At the heart of this discussion are issues of national security, foreign affairs, government regulation, and economic incentives. As Congress, you will have the power to put

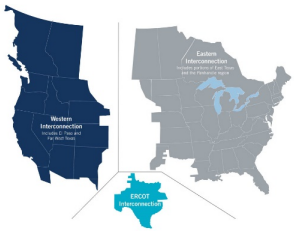
forth guidance, reorganize federal agencies, and craft legislation to shore up existing cyber defenses before the next attack.

EXPLANATION OF THE ISSUE

Critical Infrastructure *– the 16 critical infrastructure sectors defined by the cybersecurity and infrastructure security agency (CISA). (See Glossary for the full list)*

Historical Development

The development of the United States' **critical infrastructure** such as the power grid, oil pipelines, water processing system, broadband, and so forth originated as a patchwork of independent systems. In these early days, there was a minimal connection between these systems creating a decentralized network (Collins 2020). However, as technology developed and these systems became digitized, there was both a cost and efficiency perspective to connect these disparate systems into an interconnected one. For instance, the lower-48 states have three main power grids that essentially power all activity. These are the Eastern Interconnection, the Western Interconnection, and Texas (Galbraith, 2021). Although Texas may have chosen to be independent to escape federal regulations, it learned the hard way the dangers of having an independent system.



Map of the three electrical interconnections in North America.
ERCOT

In February of 2021, a fierce snowstorm combined with unusually cold temperatures crippled the state's electric grid and caused around 4.5 million Texans to lose power (Kim 2021). Normally, in an interconnected system, states can divert part of their energy supply to neighboring states in times of crisis. Unfortunately for Texas, its independence streak meant that its neighbors on all sides were unable to divert their power to the state, leaving much of the state without electricity. While there are legitimate fears of a centralized system, there are many benefits that come with an interconnected critical infrastructure network that can prove to be more resilient than a disparate patchwork.

Alongside the increase in connectivity of the United States' critical infrastructure was the rapid pace of digitization. In essence, systems were not only being connected to each other but the processes were being automated and digitized, exposing them to threats of cyberattacks. Companies are embracing this shift simply because it makes economic sense. The International Energy Agency estimates that digital technologies have the potential to increase the production of oil and gas by 5% and reduce costs by 10% (Bordoff, 2018). Morgan Stanley notes that the potential of this revolution can lead to a decline in cost not seen since the decade from 1987-1997 (Bordoff, 2018). Consumers are benefiting from this shift. Beyond cheaper gas prices, other facets of critical infrastructure such as healthcare are being improved. Electronic Health Records have improved healthcare by decreasing dosage errors, communication

Hacking incidence was up 42% compared to 2019, the fifth continuous year of increase. – (Stewart 2020)

errors and improving management of data as well as increase patient satisfaction and much more (Atasoy, 2018). The increased reliance on electronic systems is a necessity for cheaper goods and services even if it carries a certain risk.

Moreover, the rapid pace of privatization of critical infrastructure from banking to healthcare to the transport of electricity is hampering effective regulation. By 2011, it was estimated that about 85% of the nation's critical infrastructure is controlled by the private sector" (Givens, 2011). As the number of new and more complex infrastructure increases, so too will the percentage. What all three of these factors lead to is an increasingly interconnected system that is being automated and digitized even as the fractured nature of private ownership greatly inhibits meaningful government oversight. These factors are largely unavoidable and carry plenty of benefits. However, steps must be taken to ensure that the benefits conferred by these properties are not weaponized to weaken critical infrastructure.

Blackout in New York after Hurricane Sandy
New York Magazine

Scope of the Problem

The three large problems that arise from the qualities of an interconnected, digitized, and privatized infrastructure grid are: (1) magnification of breach, (2) exposure to foreign adversaries, (3) difficulty in regulation. While there are assuredly many more problems, these are key problems that any meaningful piece of legislation must solve.

Magnification of Breach

The very qualities that make an interconnected system so great, efficient and resilient, can also be one of its most critical flaws. One way to visualize this is through an analysis of a potential attack on a region's power grid. Researchers at the University of Cambridge have estimated that a potential cyberattack on just 50 generators that supply the northeast with power could trigger a wider blackout due to its connected nature leaving around 93 million people without power (Ruffle et. Al, 2015). In this hypothetical scenario which could take place, the economic impact would rise above $240 billion and possibly even up to $1 trillion in the worst-case scenario. This is because the eastern United States are all connected under one power grid; hence a malware can travel between nodes wreaking havoc. Additionally, electricity plays a critical function in all activities from manufacturing to providing quality healthcare. A disruption in the electrical grid is not just costly, it is dangerous as well.

Colonial Pipeline Attack *– a cyberattack on Colonial Pipeline Inc., by a Russian-based group, which supplies nearly half of the East Coast's oil needs.*

Turning to a more recent real-life example, the **colonial pipeline attack** mentioned previously had broader implications for the economy. Following the May 7th, 2021, attack, the average gas price jumped 6 cents per gallon, just three short of making gas the most expensive since 2014 (Bajak, 2021). In hard-hit states such as

Georgia and South Carolina, gas prices jumped by eight percent while in Washington D.C., nearly 90 percent of gas stations had "no gas" signs posted (Bordoff, 2021). This massive increase in oil and gas prices led to price increases on food and appliances as transportation and delivery of goods became more expensive (Eaton, 2021). Another factor to consider was that the attack occurred in late spring. Had the attack been during winter, many homes might have found themselves paying significantly higher heating bills. Of course, all these disruptions to the daily life of millions may be costly and inconvenient but are at least temporary. This is because the CEO of Colonial Pipeline Inc. decided to pay the whopping $5 million ransom to unlock its system. In the future, when cyber-attacks are not just carried out by hackers looking for money but by governments who want to inflict damage, there may be no ransom to be paid and the disruption permanent. When the United States' economic engine is intertwined with these critical infrastructures, any small attack can have massive consequences.

Icicles on a ceiling fan in Dallas, Texas after a snowstorm
Thomas Black

Exposure to Foreign Adversaries

While the rapid embrace of new technology such as automation and artificial intelligence (AI) has proven cost-effective for companies, it has also brought critical infrastructure into cyberspace, opening it up for cyberattacks. In the real world, robbers must physically enter a home or firm to steal from it. Governments also must physically deploy firepower to inflict physical damage on critical infrastructures such as power plants, bridges, or oil pipelines. These requirements are virtually nonexistent in cyberspace, erasing physical barriers and distances. Therefore, cyberattacks are often seen as a more effective way of committing crimes or inflict political damage.

In 2018, the Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) reported that beginning in March of 2016, Russian government hackers attempted to hack into energy, nuclear, water, manufacturing, and other commercial facilities but was effectively identified and neutralized by the agencies (Volz, 2018). This blistering report documents the danger that the United States faces from its adversaries daily. Though that effort was successful, the SolarWinds attack by Russian operatives in 2020 and the Chinese attack in 2021 proved that the United States is a long way from securing its cyberspace (Collier, 2021). With the SolarWinds attack, federal agencies such as the State Department, DHS, Treasury, and Commerce Departments as well as the Department of Defense were breached by the malware and vital data was stolen (Sanger, 2020).

These are just two examples of foreign governments weaponizing cyberspace and exploiting critical security vulnerabilities in the United States' infrastructure.

Difficulty in Regulation

Companies often balk at the cost of securing the infrastructure that they are responsible for, since very expensive cyber defenses can be breached.

Infrastructure in the United States is primarily owned by the private sector which makes oversight and regulation difficult. This is primarily because of a lack of a strong incentive for companies to adequately shore up their defenses. According to Fred Cate, the director of the Center for Applied Cybersecurity Research, an inequality of knowledge levels between companies as well as the incentive to maximize profit stand in the way of a robust market-based response to the rise in cybersecurity threats (Etzioni, 2011). Simply put, the inequality of knowledge levels about cyber defense between companies is a source of competition, where firms may not have an incentive to share critical information with other firms. Companies that boast robust security apparatus can gain over customer's trust and those that hide critical information from consumers can prevent large losses.

Cybersecurity investment is incredibly expensive with many robust firewall and monitoring systems amounting to hundreds of thousands to millions of dollars (Debar, 2019). All of this investment in cyber defense may prove futile as demonstrated by the Colonial Pipeline Hack. The company had spent around $200 million in cybersecurity, yet it was crippled by ransomware (Eaton, 2021). What this illustrates is that the cost and occasional ineffectiveness of current cyber defense systems are disincentivizing companies to invest in them.

The final issue stemming from the private sector is their unwillingness for stricter regulation. Businesses fear that forcing companies to adopt stricter standards may harm their ability to innovate. Furthermore, companies view the issue of securing national assets as a public-sector responsibility, to be shouldered by the government, not private firms. For legislation to be effective, strong economic incentives for firms or strong regulations are needed.

Cybersecurity and Infrastructure Security Agency (CISA) *– an agency created by President Trump, under control of the Department of Homeland Security, tasked with resolving cyberthreats and securing critical infrastructure.*

Congressional Action

Over the years, Congress has passed a variety of legislation to combat cyber threats. The Homeland Security Act of 2002 gave the DHS cybersecurity responsibilities to bolster protection for critical infrastructure (Fischer, 2014). This act made the DHS the de-facto leader for civilian cyber defense. The Cyber Security Research and Development Act of 2002 gave responsibility and funding to the National Science Foundation and the National Institute of Standards and Technology to research more effective methods of combatting cyberthreats (Fisher, 2014). These two acts along with many others were the early steps the United States took to improve cyber defenses. More recently, President Trump signed into law the Cybersecurity and Infrastructure Security Agency Act of 2018 which

established an agency under the DHS's umbrella with the same name as the act (CISA). **CISA** is tasked with identifying and resolving cyber threats along with securing the nation's critical infrastructure (Congress, 2018).

Although there are many other smaller pieces of legislation designed to encourage increased research, investment, and regulation of cyber defenses, there is still no federal cybersecurity law with general application. The majority of regulations imposed on businesses are either sector-specific (and tend to be passed in a reactionary manner) or state laws (McNicholas et. Al, 2021). This results in a lack of a single framework for non-compliance by businesses (McNicholas et. Al, 2021). The hodgepodge of various federal, state, and local laws creates an insufficient regulatory framework for efficient oversight.

IDEOLOGICAL VIEWPOINTS

Traditionally, both sides are in support of improving cyber defense systems, especially when it comes to protecting critical infrastructure. However, there are sharp divisions when it comes to solutions. To put it simply, the clash comes down to the role of government in cybersecurity.

Conservative View

Conservatives tend to favor a market-oriented, incentive-based approach over stringent federal regulations (Inzaurradle, 2018). They are strong proponents of establishing a federal security standard instead of a mandate that allows for businesses to make their own decisions regarding the matter. With that said, there have been some voices of support for an increase of skilled cybersecurity-trained civilian personnel. Senator Marsha Blackburn (R-TN) for instance has co-sponsored legislation with Senator Jacky Rosen (D-NV) regarding the creation of a civilian cybersecurity reserve program (Moran, 2021).

In the past, Republicans have championed legislation such as the SECURE IT Act which was introduced in 2012 (Congress, 2012). Though it did not pass, it can give some insight into the conservative approach to cybersecurity. It allows private entities to collect and identify information related to cyber threats, however, the government cannot use such information to regulate a firm's activities. Additionally, it encourages the sharing of information between entities of the public and private sectors. The legislation would have established a scholarship and training program to incentivize more people to enter the cybersecurity field (Congress, 2012). In short, the conservative view on this matter gives the

government the role of providing incentives for firms as well as the labor market to invest in and share knowledge of cyber defenses.

Liberal View

Liberals tend to favor the centralization of cybersecurity defense and response. Then-President Obama created the position of Federal Chief Information Security Officer. They are tasked with cybersecurity planning and implementation in the government. (White House, 2016). This push has continued in 2020 with the introduction of the National Cyber Director Act in the House (Congress, 2020). This act would form a new Office of National Cyber Director, who will assist in the development and implementation of federal responses to cyber-attacks. This act later became a provision in the Defense Authorization Act of 2021. It is a clear push to take a more centralized approach instead of leaving it up to the various agencies.

Then President Obama speaks at a Summit on Cybersecurity and Consumer Protection and outlining his agenda.
Stanford University

Besides centralization, liberals want the government to directly invest in the IT infrastructure necessary to defend against cyberattacks. President Obama's 2017 budget proposed a $3.1 billion IT Modernization Fund, $62 million in cybersecurity training, and a total of $19 billion for cybersecurity (White House, 2016). This has continued under President Biden who has pushed for increased spending in cybersecurity. In his budget for 2022, Biden proposed nearly $9.8 billion in cybersecurity funding to protect existing infrastructure (OMB, 2021).

Finally, instead of the implementation of standards as proposed by Republicans, Democrats want to impose strict mandates for the private sector. They have pushed for new laws that would raise financial penalties for data breaches, and mandate reforms on consumer notification (Inzaurralde, 2018). In short, Democrats prefer a more robust government response that would regulate and fund efforts to improve cybersecurity.

AREAS OF DEBATE

Centralize Response to Cyberattacks

There appears to be a bipartisan push for a more streamlined response process from both sides of the aisle, making this one of the more feasible options to implement. Findings conducted by NIAC point to a division in cybersecurity capabilities. This division leads to difficulty in coordination and many agencies play duplicative roles (NIAC, 2018). There are six federal cybersecurity centers, 140 cyber authorities spread across 20 agencies, and eight different assessment programs. This web of complexity highlights the difficulty in preparing a coordinated response when it comes to attacks on critical

infrastructure. Beyond the bureaucratic nature of the current system, the privatized nature of the United States' critical infrastructure makes coordinating with the private sector a necessity. The labyrinth of different agencies disincentivizes the private sector from fully cooperating with the government which can be detrimental to national security.

Many believe that the best way to address this is to create a new position or agency at the national level dedicated to cybersecurity that can recommend policy, coordinate efforts between the public and private sector, and implement cybersecurity reforms and policies. Supporters believe that this new agency would improve coordination, boost efficiency, and make it easier for regulations to be monitored and implemented. Additionally, there would a singular agency that Congress can maintain oversight on the progress made. Detractors believe that this is a clear government overreach. However, many fear that this new agency will be emboldened to regulate private industries, stifling innovation, and slowing economic growth. Additionally, the creation of a new office or agency would serve to expand the size and role of government in daily life.

Chris Inglis has been chosen by President Biden as the first national cyber director.
New York Times

Political Perspectives on this Solution

In the past, this has been more of a liberal policy proposal, however, the increasing threat of cyberattacks has prompted support for the idea from both sides. In fact, the National Cyber Director Act introduced in 2020 was sponsored by congressional members from both sides of the aisle. With that said, there are differences held on both sides regarding the powers of the position.

For instance, some believe that creating a separate office or agency undermines the interconnected nature of the various agencies, excluding key players from the conversation (O'Connell, 2020). Additionally, the private sector has indicated their preference to have a wide variety of options when coordinating with the government, since some sectors are more suited to a particular agency. It would also be an expansion of government which is not particularly appealing to conservatives. This view is rather rare and only held by the most conservative members of congress. Many Republicans are in support of this centralization effort although they would prefer the agency to play less of a regulatory role.

Democrats on the other hand are in favor of this proposal through their actions mentioned previously. Overall, this plan has a very good chance of achieving bipartisan appeal, yet there are still minor conflicts to work out regarding the power and role of the agency.

Economic Incentives

This approach is more market-oriented than the previous one. It suggests that economic incentives such as relief from audits, limited-

Economic incentives can be a much more flexible and easy solution for businesses to adopt new cyber defenses.

time tax credit, and access to grants and investments from the government can quicken the adoption of new cybersecurity measures. Instead of being mandated by the government, private firms can do what is best for their business and take advantage of the economic incentive (NIAC, 2018).

Government mandates tend to be unattractive to the private sector since it is not a one-size-fits-all regulation. Many firms may find themselves overprepared or overburdened by regulations that may not apply to the business that they are running. Regulations also are reactionary measures that have a difficult time keeping up with the times, since regulatory legislation faces immense scrutiny when passing through congress. This makes for a regulatory system that is very slow to update and ineffective at keeping up with the speed of technological progress.

Another problem that this solution addresses is cost, one of the greatest issues for companies is the cost of maintaining a strong cyber defense. If the government can provide some relief for firms that maintain the nation's critical infrastructure, they will be able to update their defenses more frequently.

A proposal to provide financial incentives to electric utilities who went above mandatory cybersecurity standards was divisive. Investor-owned utilities embrace the idea while public power companies balked at it.

While proponents cite the benefits above, opponents view the push for a market-oriented approach as inefficient. Companies may exploit the system leading to minimal improvement. There are many other potential usages for funds such as increased funding for cybersecurity training and education.

Political Perspectives on this Solution

This approach is more likely to be embraced by large businesses and conservative members of congress. In 2011, a Republican Taskforce on cybersecurity encouraged the usage of tax and economic incentives to nudge businesses to adopt up-to-date cybersecurity practices (Gross, 2011). Moderate Democrats have also joined the Republicans in supporting this measure, but they would prefer to have additional regulations alongside the economic incentives.

The RAND institute noted that existing financial incentives for security are insufficient (Weinbaum, 2018). One of the biggest issues with current incentives is the potential increase in cost to consumers that arises. Economic incentives could lead businesses to implement changes that may be unnecessary or incompatible to exploit tax incentives which could increase the price of goods and services on up (Melvin, 2021). Overall, there is some liberal opposition to this proposal, but it remains reasonably popular with lawmakers on both sides.

Impose Federal Regulations

The United States lacks a general regulatory framework for tackling cyber threats. This has led to plenty of finger-pointing by

various stakeholders. Individuals point to institutions for security failures but are then blamed by firms for wanting low prices. Firms blame the government for insufficient protection and the government blames firms for providing an insecure product (Weinbaum, 2018). This vicious cycle of blame makes the need for strong regulations. It is important to remember that consumers do not like high prices and companies do not like to incur more expenses than they must. Therefore, the result is an insecure world. This is one of the main flaws in a market-oriented approach.

A robust set of government mandates and regulations can help bridge this gap according to those in favor of the idea. The first appeal is to streamline current regulations. At the state level, regulations vary wildly with some having strict mandates while others prefer a looser approach. This leads to a hodgepodge of potentially contradictory regulations as critical infrastructure spans multiple states. Since there is a lack of regulation at the federal level, businesses have largely ignored or failed to adhere to the minimum standards. Mandates for private and public entities to share information, submit to audits and keep up to date with new cyber defense technology may be effective at keeping critical infrastructure safe.

A flyer put out by the Federal Virtual Training Environment (FedVTE) to encourage government employees to undergo complimentary cybersecurity training.

FedVTE

Opponents of the idea believe that federal regulations will serve as a burden, not as a shield. This is because regulations can be a cost burden to growing firms which could slow down competition. Additionally, regulations may end up not solving the rising cost situation since companies will have to pay more for increased security, passing the cost onto consumers.

Political Perspectives on this Solution

As mentioned previously, regulations tend to be opposed by conservatives. They view the government and the bureaucracy that will inevitably rise to enforce federal regulation to be less effective than market-oriented approaches. Private businesses would also prefer an alternative approach since they do not want to be shouldered with extra cost. With this in mind, any federal regulation should balance both the liberal perspective of keeping private entities accountable while addressing the potential loss of innovation and higher costs that conservatives fear.

Training and Development

Unlike many other proposals, the belief that the government should increase funding, either through grants or scholarships to train the next generation of cybersecurity experts. The United States currently lacks about half a million workers to meet the rising demand for cybersecurity expertise (Rogers, 2020). There is a real talent gap of minority groups in the industry (Rogers, 2020).

One of the best solutions is to offer educational scholarships to students, which can be authorized through funding of the Department of Education. Additionally, grants can be offered by the National Science Foundation to lessen the cost of training employees for private businesses. These are some potential solutions.

The crux of the debate on the implementation tends to focus on where the money should be allocated and how much.

Political Perspectives on this Solution

There is broad consensus on both sides of the aisle on this matter. In the past, bipartisan legislation has been introduced and passed in both chambers to increase funding for education and training. The debates here boil down to whether funds should be provided to college students wishing to study Information Technology or Computer Science to prepare them for a career in the field or to firms to train their employees. There is no true political divide on this matter, just different priorities for different members of congress.

International Cooperation

A meeting on cybersecurity at the United Nations Office for Disarmament Affairs

United Nations

Thus far, the discussion has largely revolved around preparing for the next cyber-attack on critical infrastructure, however, to really mitigate attacks from foreign adversaries, international cooperation is required. The Council on Foreign Relations (CFR) notes that there is a misconception of believing that the primary source of attacks comes from foreign governments. In fact, in the digital age, cyberattacks are often carried out by non-state actors such as thieves looking to make money (CFR, 2018). Here, global economies are vulnerable, providing common ground for dialogue.

Some suggestions provided by the CFR are to restart the U.S.-Russia dialogue on cyber issues (CFR, 2018). This is because cyber warfare should be treated the same as a conventional war, where a "non-aggression pact" may yield beneficial results for both sides. This has worked in the past in the case of the non-aggression pact signed by China and the United States in 2015. In fact, one year following the pact, the number of network compromises by Chinese-based groups dropped to 10%, down from 60% three years earlier (Segal, 2016). It is important to remember that it is not impossible to find some common ground among political adversaries.

Another place where international cooperation can prove to be beneficial is to work on a UN resolution mandating member states to report cyber vulnerabilities (CFR, 2018). By working to create an international framework for coordination and prosecution of violators, the global cyberspace will be safer. Vulnerabilities discovered in one member state can be used to improve global security.

Cooperation with foreign adversaries may be used by those on the opposite side of the political spectrum as a sign of weakness.

While the potential benefits are great, there are many who are opposed to some of these ideas, especially the last part of creating and joining an international framework for the reporting of vulnerabilities. By sharing knowledge of vulnerabilities, national security could be undermined. Also, if the United States has to adhere to a global standard, many will view this as a loss of sovereignty. Working with China and Russia is not particularly popular on both sides of the aisle. For liberals, Russia was the country that attempted to undermine the 2016 election. For conservatives, China is the new adversary on the global stage and must be distrusted. To find common ground here is difficult. Finally, the funding required to help developing member states bring their IT infrastructure up to the global standard will require contributions from the United States, something that conservatives view unfavorably. These are some of the potential issues that need to be addressed if this option were to be implemented.

Political Perspectives on this Solution

Conservatives believe China is the biggest threat, likely due to Trump's rhetoric, while liberals believe Russia pose the greatest threat, likely due to Biden's tough stance.

Liberals tend to be more favorable towards multilateralism while conservatives believe that international organizations work to undermine the United States' interests (Call, 2016). For Democrats, 87% are in support of increasing support with allies on the international stage, only 48% of Republicans do (Pew Research Center, 2020). This divide also extends to the question of which country is the greatest threat to national security. According to a YouGov poll, only 14% of Democrats view China as the biggest threat, compared to 40% for Russia (Frankovic, 2021). As for Republicans, only 8% view Russia as the biggest threat compared to 54% for China (YouGov, 2021). This divide will make it difficult for partnerships with either of these countries to coordinate cybersecurity efforts. Overall, the view surrounding international cooperation is polarizing and legislation should try to bridge some of this divide.

BUDGETARY CONSIDERATIONS

As Congress, you have full control over the crafting of the federal government's budget. However, under Article 1 of the United States constitution, all legislation concerning the budget and funding must originate from the House of Representatives. With that said, senators are allowed to push for funding of certain provisions if they can convince the House to go along with it. There are two considerations when thinking about the budget. The first is the national debt and the second is taxes. In order to pay for the provisions you laid out, the federal government must either reallocate funds from other agencies, raise taxes, or deficit spend. As of June of 2021, the national

debt is $28 trillion dollars which equates to a debt to GDP ratio of 128% (US Debt Clock, 2021). Though interest rates are extraordinarily low, and have been for a very long time, they may increase in the future which could dramatically increase the debt burden placed on the federal government. Conservative members are likely to be weary of raising taxes or deficit spending, while more liberal members might see the future economic return of protecting critical infrastructure may outweigh the cost incurred in the present, hence raising taxes or deficit spending may be needed.

CONCLUSION

Graph of debt-to-GDP ratio over the last 50 years. It is currently at the highest level since World War II.

FRED

In an increasingly digitized world, the need for comprehensive action is now. It is vital that the United State shore up defenses for its critical infrastructure before the next attack as recognize the inherent danger of an overly interconnected system, as any disruption will be greatly magnified. In this climate, there is a severe shortage of cybersecurity personnel capable of identifying and neutralizing threats. Combine that with an overly bureaucratic government with responsibility spread across a myriad of agencies and any coordination on cybersecurity proves to be challenging. There is also an immense cost burden on companies looking to secure their system, something that needs to be addressed considering the privatized nature of the country's critical infrastructure. Finally, the digitalization of systems has opened the floodgates for attacks by foreign adversaries and non-state actors alike.

When crafting policy solutions, there is no clear single answer. As provided by this briefing, the solutions each carry drawbacks of their own, something that must be weighed in debate. For representatives to be successful, it is important to find a compromise, potentially combining and modifying existing policy with new ideas, and take both political division and budgetary constraints into consideration. In short, a thorough read of this briefing along with outside research will help representatives be successful in finding the combination of solutions to help improve national security and defend the nation's critical infrastructure.

GUIDE TO FURTHER RESEARCH

This briefing should provide a brief overview of the cybersecurity challenges, especially those relating to critical infrastructure, that the United States faces today. However, for representatives to be successful, outside research is needed. For the sake of simplicity, many issues and solutions have been left out of this briefing.

Therefore, to stay on top of legislative activity, representatives are encouraged to utilize Congress.gov to better understand the legislation proposed. Cybersecurity breaches occur frequently and thus it is essential to keep up to date on new developments. Adhere to news sources such as The New York Times, The Wall Street Journal, or the Associated Press. The Council on Foreign Relations is a great resource to understand advancement on any international cooperation efforts. Finally, senators should familiarize themselves with the various agencies and their roles in cyber defense. Visit the website DHS, NSF, CEA, and NIAC for more information.

GLOSSARY

Critical Infrastructure – The 16 infrastructure sector defined by CISA as vital to national and economic security.

1. Chemical Sector
2. Commercial Facilities
3. Communications
4. Critical Manufacturing
5. Dams
6. Defense Industrial Base
7. Emergency Services
8. Energy
9. Financial Services
10. Food and Agriculture
11. Government Facilities
12. Healthcare and Public Health
13. Information Technology
14. Nuclear
15. Transportation
16. Water

Colonial Pipeline Attack – a cyberattack on Colonial Pipeline Inc., by a Russian cybercrime group, which supplies nearly half of the East Coast's oil needs. It was estimated that DarkSide, the cybercrime group, extorted roughly $5 million from the company.

Cybersecurity – The protection of internet-connected systems from threats online. This can include hardware, software, and data.

Cybersecurity and Infrastructure Security Agency (CISA) – an agency created by President Trump, under control of the Department of Homeland Security, tasked with resolving cyberthreats and securing critical infrastructure**.**

BIBLIOGRAPHY

Atasoy, Hilal, et al. "The Digitization of Patient Care: A Review of the Effects of Electronic Health Records on Health Care Quality and Utilization." *Annual Review of Public Health*, vol. 40, no. 1, 2019, pp. 487–500., doi:10.1146/annurev-publhealth-040218-044206.

Bajak, Frank, and Cathy Bussewitz. "EXPLAINER: Why the Colonial Pipeline Hack Matters." *AP NEWS*, Associated Press, 11 May 2021, apnews.com/article/europe-hacking-government-and-politics-technology-business-b2a867c0705acd953c90d6e2a58fabb9.

Bordoff, Jason. "How AI Will Increase the Supply of Oil and Gas- and Reduce Costs." *The Wall Street Journal*, Dow Jones & Company, 3 May 2018, www.wsj.com/articles/how-ai-will-increase-the-supply-of-oil-and-gasand-reduce-costs-1525345814.

Call, Charles T., et al. "Is the UN a Friend or Foe?" *Brookings*, Brookings, 4 Oct. 2017, www.brookings.edu/blog/order-from-chaos/2017/10/03/is-the-un-a-friend-or-foe/.

Collier, Kevin. "China behind Another Hack as U.S. Cybersecurity Issues Mount." *NBCNews.com*, NBCUniversal News Group, 22 Apr. 2021, www.nbcnews.com/tech/security/china-another-hack-us-cybersecurity-issues-mount-rcna744.

Collins, Stuart. "Cyber Attacks on Critical Infrastructure." *AGCS Global*, AGCS Global, 2016, www.agcs.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html.

Eaton, Collin, and Dustin Volz. "WSJ News Exclusive | Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom." *The Wall Street Journal*, Dow Jones & Company, 19 May 2021, www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636.

Eaton, Collin, et al. "Colonial Pipeline Shutdown Threatens to Magnify Gasoline-Price Surge." *The Wall Street Journal*, Dow Jones & Company, 10 May 2021, www.wsj.com/articles/as-colonial-pipeline-shutdown-drags-on-after-hack-eyes-are-on-gasoline-prices-11620660258.

Etzioni, Amitai, et al. “Cybersecurity in the Private Sector.” *Issues in Science and Technology*, 4 May 2021, issues.org/etzioni-2-cybersecurity-private-sector-businesses/.

Fischer, Eric. “Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation.” *Crs.gov*, Congressional Research Service , 12 Dec. 2014, crs.gov.

Frankovic, Kathy. “America's Greatest Enemy, According to Republicans and Democrats.” *YouGov*, YouGov, 8 Mar. 2021, today.yougov.com/topics/international/articles-reports/2021/03/08/americas-greatest-enemy-poll.

Galbraith, Kate. “Texplainer: Why Does Texas Have Its Own Power Grid?” *The Texas Tribune*, The Texas Tribune, 8 Feb. 2011, www.texastribune.org/2011/02/08/texplainer-why-does-texas-have-its-own-power-grid/.

Gross, Grant. “Republicans Call for Voluntary Cybersecurity Incentives.” *Computerworld*, IDG News Service, 5 Oct. 2011, www.computerworld.com/article/2737933/republicans-call-for-voluntary-cybersecurity-incentives.html.

Kim , Sunny. “How Texas' Tough Winter Exposed U.S. Power Grid Problems.” *CNBC*, CNBC, 26 Mar. 2021, www.cnbc.com/2021/03/26/how-texas-tough-winter-exposed-us-power-grid-problems-.html.

McCain, John. “H.R.1468 - 113th Congress (2013-2014): SECURE IT.” *Congress.gov*, United States Congress, 24 June 2013, www.congress.gov/bill/113th-congress/house-bill/1468.

Melvin, Jasmin. “Power Industry Divided over FERC's Proposed Incentives for Cybersecurity Measures.” *S&P Global Platts*, S&P Global Platts, 7 Apr. 2021, www.spglobal.com/platts/es/market-insights/latest-news/electric-power/040721-power-industry-divided-over-fercs-proposed-incentives-for-cybersecurity-measures.

Moran, Cooper. “Senator Marsha Blackburn Calls for New Cybersecurity Measures.” *Tennessee Star*, 12 May 2021, tennesseestar.com/2021/05/12/senator-marsha-blackburn-calls-for-new-cybersecurity-measures/.

O’Connell, Sasha Cohen. “Opinion: We Don't Need a Separate Cybersecurity Agency.” *POLITICO*, POLITICO, 29 Jan. 2020, www.politico.com/news/agenda/2020/01/29/dont-need-separate-cybersecurity-agency-106631.

Pew Research Center. "2. Political Values and Democratic Candidate Support Political Values and Democratic Candidate Support." *Pew Research Center - U.S. Politics & Policy*, Pew Research Center, 2 Oct. 2020, www.pewresearch.org/politics/2020/01/30/political-values-and-democratic-candidate-support/.

President National Infrastructure Advisory Council. "Securing Cyber Assets ." *Cisa.gov*, Cybersecurity and Infrastructure Security Agency, Aug. 2017, www.cisa.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf.

Rogers, Kate. "'We Are Outnumbered' - Cybersecurity Pros Face a Huge Staffing Shortage as Attacks Surge during the Pandemic." *CNBC*, CNBC, 6 Sept. 2020, www.cnbc.com/2020/09/05/cyber-security-workers-in-demand.html.

Ruffle , Simon. "Lloyd's Business Blackout Scenario." *Cambridge Judge Business School*, 19 Nov. 2020, www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/technology-and-space/lloyds-business-blackout-scenario/.

Sanger, David E., and Nicole Perlroth. "Russia Appears to Carry Out Hack Through System Used by U.S. Aid Agency." *The New York Times*, The New York Times, 28 May 2021, www.nytimes.com/2021/05/28/us/politics/russia-hack-usaid.html.

Sanger, David E., et al. "Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit." *The New York Times*, The New York Times, 15 Dec. 2020, www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html.

Segal, Adam. "Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms." *Council on Foreign Relations*, Council on Foreign Relations, 28 Sept. 2016, 9:00, www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms.

Stewart, Angie. "Key Takeaways from the 2021 Breach Barometer." *Blog*, Poteneus, 15 Mar. 2021, blog.protenus.com/key-takeaways-from-the-2021-breach-barometer.

US Debt Clock. *U.S. National Debt Clock : Real Time*, 2021, www.usdebtclock.org/.

Volz, Dustin, and Timothy Gardner. "In a First, U.S. Blames Russia for Cyber Attacks on Energy Grid." *Reuters*, Thomson Reuters, 15 Mar. 2018, www.reuters.com/article/us-usa-russia-sanctions-energygrid/in-a-first-u-s-blames-russia-for-cyber-attacks-on-energy-grid-idUSKCN1GR2G3.

The Washington Post. "The Cybersecurity 202: Republicans and Democrats Are Feuding over the Equifax Breach." *The Washington Post*, WP Company, 17 July 2020, www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/12/11/the-cybersecurity-202-republicans-and-democrats-are-feuding-over-the-equifax-breach/5c0e9ec91b326b67caba2b5c/.

Weinbaum, Cortney, et al. "Financial Frameworks for Cybersecurity Are Failing." *RAND Corporation*, Rand Corporation, 25 Oct. 2018, www.rand.org/blog/2018/10/financial-frameworks-for-cybersecurity-are-failing.html.

The White House. "FACT SHEET: Cybersecurity National Action Plan." *National Archives and Records Administration*, National Archives and Records Administration, 2016, obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

Image Credit

Baan, Iwan. "Blackout in New York after Hurricane Sandy." *New York Magazine*, New York Magazine, 3 Nov. 2012, images.nymag.com/news/features/sandy121105_intro_560.jpg.

Black, Thomas. "Icicles Hang from Ceiling Fan after a Cold Snap in Dallas, Texas." *USA Today*, USA Today, 17 Feb. 2021, www.gannett-cdn.com/presto/2021/02/17/USAT/ab5291df-c1af-4e80-970a-46eb08c150cb-icicles_from_fan.jpeg?crop=1536,1553,x0,y328&width=300&height=304&format=pjpg&auto=webp.

Cicero, Linda. "President Barack Obama Onstage at the White House Summit on Cybersecurity and Consumer Protection on Feb. 13." *Stanford Foreign Institute for Foreign Studies*, Stanford University, 13 Feb. 2015, cisac.fsi.stanford.edu/news/obama-stanford-ceos-must-commit-cyber-security.

Cyrus, Logan. “Attendants Directed Cars as They Lined up to Fill Their Gas Tanks in Charlotte, N.C., on Tuesday.” *The New York Times* , The New York Times , 5 May 2021, static01.nyt.com/images/2021/05/11/business/11pipeline2/merlin_187603953_a5119945-5552-4438-b7c1-b968d3cb8957-jumbo.jpg?quality=90&auto=webp.

Dharapak, Charles. “Chris Inglis, a 28-Year Veteran of the National Security Agency Who Has Been Chosen by President Biden as the First National Cyber Director.” *The New York Times*, The New York Times, 21 Apr. 2021, static01.nyt.com/images/2021/04/12/us/politics/12dc-cyber/merlin_186301347_05577f04-8c21-4604-91c9-3d8fcb3f3818-jumbo.jpg?quality=90&auto=webp.

Electric Reliability Council of Texas. “The Three Main Components of the North American Power Grid Are the Western and Eastern Interconnections and the ERCOT Interconnection, managed by the Electric Reliability Council of Texas and Encompassing Most of the State.” *Yale Climate Connections*, Yale University, 17 Feb. 2021, i0.wp.com/yaleclimateconnections.org/wp-content/uploads/2021/05/0221_ERCOT-Internconnection_Branded.jpg?w=974&ssl=1.

FedVTE. *FedVTE*, Federal Virtual Training Environment. , 2021, niccs.cisa.gov/sites/default/files/documents/pdf/fedvte_flyer.pdf?trackDocs=fedvte_flyer.pdf.

Federal Reserve Bank of St. Louis. “Debt-to-GDP Ratio over Time. .” *FRED* , Federal Reserve Bank of St. Louis , Dec. 2020, fred.stlouisfed.org/graph/fredgraph.png?g=lGiW&nsh=1&width=600&height=400&trc=1.

