Forum for American Leadership

Eight Necessary Steps to defend U.S. Critical Energy Infrastructure from Cyber Attacks

October 4, 2021

A prolonged disruption in energy flows caused by foreign cyberattackers could quickly inflict catastrophic harm to American lives, health, and national security. The May 7, 2021, Colonial Pipeline cyberattack highlighted the importance of engaging in strategic deterrence against future, potentially catastrophic, attacks on our critical energy infrastructure and exposed significant national security gaps that require timely legislative and executive branch remedies. Congress must work with the Executive Branch to take robust steps to deter and punish cyberattacks on critical energy infrastructure while preparing the country to manage future attacks better than it did in May. Actions to date have fallen far short.

Recommendations for Congress to restore deterrence and bolster our domestic defense:

1. Toughen penalties and sanctions for foreign cyber attackers who target critical energy and other vital U.S. infrastructure.

2. The United States should deter, preempt, and punish foreign cyber attackers targeting U.S. critical energy infrastructure as it would Al Qaeda, ISIS, or any other similar foreign-based terrorist planning or using WMD to inflict catastrophic harm to the homeland and Congress should provide additional clear authority, funding, and direction to the Executive Branch to do so.

3. Require the President to notify Congress of countries that support cyber attackers who have, are, or are likely to plan or execute cyberattacks against critical energy infrastructure.

4. To prevent a loss of deterrence, Congress should first require the President to immediately formulate and implement a more robust and cyber defense and offense strategy. Elements of such a strategy should include bolstering our active defense, persistent engagement between the executive and legislative branches and with our allies and defend-forward efforts. Likewise, it should provide clear authority, funding and direction for activities that go beyond such efforts in the case of further attacks on critical energy infrastructure. In addition, the President should be required to inform Congress of the Administration's implementation progress no later than six months after completion, and upon submission, Congress should allocate additional funds to ensure swift and safe implementation of the new strategy.

5. Declare it shall be the policy of the United States to regard any future attempts to disrupt or dismantle U.S. critical energy infrastructure by cyber attackers an act of aggression that shall warrant swift and commensurate retaliation against the attackers and any foreign governments deemed to sponsor them.

6. The federal government should spend more money on human capital and training for public-private cybersecurity programs, which will improve the government's capacity to help companies that are managing critical energy infrastructure assets. Specifically, federal agency representatives should embed with the nation's most essential infrastructure nodes to facilitate intelligence and real-time information sharing on industrial security threats (including attacker methodologies) and defensive countermeasures, as well as to create the ability for the government and industry to collaborate in real-time prior to, during, and in the aftermath of a potential attack.

7. Require critical energy infrastructure owner-operators to immediately inform the federal government of major cyber or any other type of attacks that could impact domestic supply. TSA has mandated reporting for pipelines, but Congress should provide incentives—like liability and regulatory protection to encourage robust and rapid reporting. Reporting mandates should protect the identity of reporting organizations and provide liability and regulatory protection.

8. Require the owner-operator of a critical energy infrastructure asset to consult and obtain the permission of the appropriate federal authority before taking any discretionary action, including the prolonged shutdown of energy flows, that could threaten the economy or national security. Provide an exception in cases when operators do not have sufficient time to consult with federal officials, i.e., to prevent a chain reaction, leak, staving off an ongoing attack, or the like. Normally, the appropriate initial response to a detected cyberattack is to immediately shut down the asset to contain and assess damage. Normally, the federal government should not dictate how private companies operate. However, in the case of a foreign attacks on vital energy infrastructure that could quickly inflict catastrophic damage to the homeland, the federal government must have the final say about whether to implement any prolonged, discretionary shutdown of critical energy flows.

Analysis and Further Information:

The Russian-based attack on the Colonial Pipeline differed critically from the thousands of prior cyberattacks on U.S. persons, businesses, and government agencies. For the first time, foreign attackers directly, if temporarily, disrupted physical energy flows vital for the societal functioning and national security of the United States. The pipeline supplies 45-50% of East Coast liquid fuel supplies, 90 military bases and installations, and seven major airports. The Colonial Pipeline attack resulted in by far the biggest loss of domestic energy supplies due to hostile foreign action against the U.S. homeland.

The most dangerous consequence of the Colonial Pipeline attack, if it is not met with an appropriate response, could be the loss of strategic deterrence. If adversaries believe they can attack critical energy infrastructure without significant cost, further and more extensive attacks are likely. Because energy storage is limited, a prolonged disruption in electricity and liquid fuels would quickly cascade into other critical sectors, inflicting catastrophic harm on American health, public safety, and national security. The Cybersecurity and Infrastructure Security Agency noted in November 2019:

> Energy stakeholders provide essential power and fuels to stakeholders in the communication, transportation, and water sectors, and, in return, the energy sector relies on them for fuel delivery (transportation), electricity generation (water for production and cooling), as well as control and operation of infrastructure (communication).

The Colonial Pipeline attack requires that national leaders review and revise how we protect the homeland from the mounting and dangerous threat posed by foreign cyber attackers. The Constitution assigns responsibility for protecting the homeland from foreign attack to the President as commander-in-chief. At the same time, Congress has a role to play through its constitutionally assigned roles as the body responsible for raising and supporting military forces and authorizing war. Cyberattacks are a potentially lethal and increasingly common means for foreign enemies to attack the United States. A weak or incomplete response to the Colonial Pipeline attack, and failure to rectify the weaknesses and vulnerabilities it exposed, would invite further attacks with potentially devastating consequences. The President has so far not demonstrated that Russia – the state that harbored the Colonial Pipeline attackers – will pay any substantive price nor taken any public action to deter future attacks other than public statements and a conversation with Russia's leadership that doesn't appear to have had any substantive impact.

While investigation is still ongoing, public reports and five congressional hearings have already revealed the attack exposed important challenges in how with address cyberattacks targeting critical energy infrastructure. For example, the federal government was neither informed nor consulted about Colonial Pipeline's decision to pay the ransom, despite FBI recommendations against victims doing so, nor was it consulted beforehand about Colonial Pipeline's decision to protect the pipeline systems by shutting it down temporarily.

There are legitimate concerns about what role the federal government should play in directing how a private company operates its assets, including when to shut down or pay ransom in response to a cyberattack. However, in the case of foreign cyberattacks *on critical energy infrastructure*, the federal government's responsibility to protect the homeland suggests that, at a minimum, the government ought to be consulted when such major actions are taken with respect to such systems, particularly given the enormous potential harm a prolonged energy outage poses to American lives, health, and national security.

Since May, Congress and the Biden administration have taken some reasonable, if only preliminary, steps. They include:

- On May 12, President Biden issued an Executive Order aimed at improving cybersecurity and federal government networks.
- On May 27, DHS issued a security directive that required critical pipeline owners and operators to report confirmed and potential cybersecurity incidents to the federal government.
- On July 20, a second DHS security directive required further steps by hazardous liquids and natural gas pipeline companies.
- On July 28, President Biden signed a National Security Memorandum directing various vanilla interagency actions.
- Several bills working their way through the House and the Senate aim to improve cybersecurity after the Colonial Pipeline attack. They would increase requirements for private companies to report on cybersecurity incidents and provide funding for states and local governments to increase cybersecurity measures.

These measures fall far short of addressing some of the challenges noted above.   Bolstering our defenses against catastrophic attacks on critical energy infrastructure requires clear and robust legislative changes that establish clear thresholds for the U.S. response.

The Forum *for* American Leadership *(FAL) is a non-profit organization that presents expert analysis and national security recommendations to policymakers in Congress and the Executive Branch.*

Want to learn more about this subject, arrange an interview, or set up a briefing with FAL experts? Contact us here.