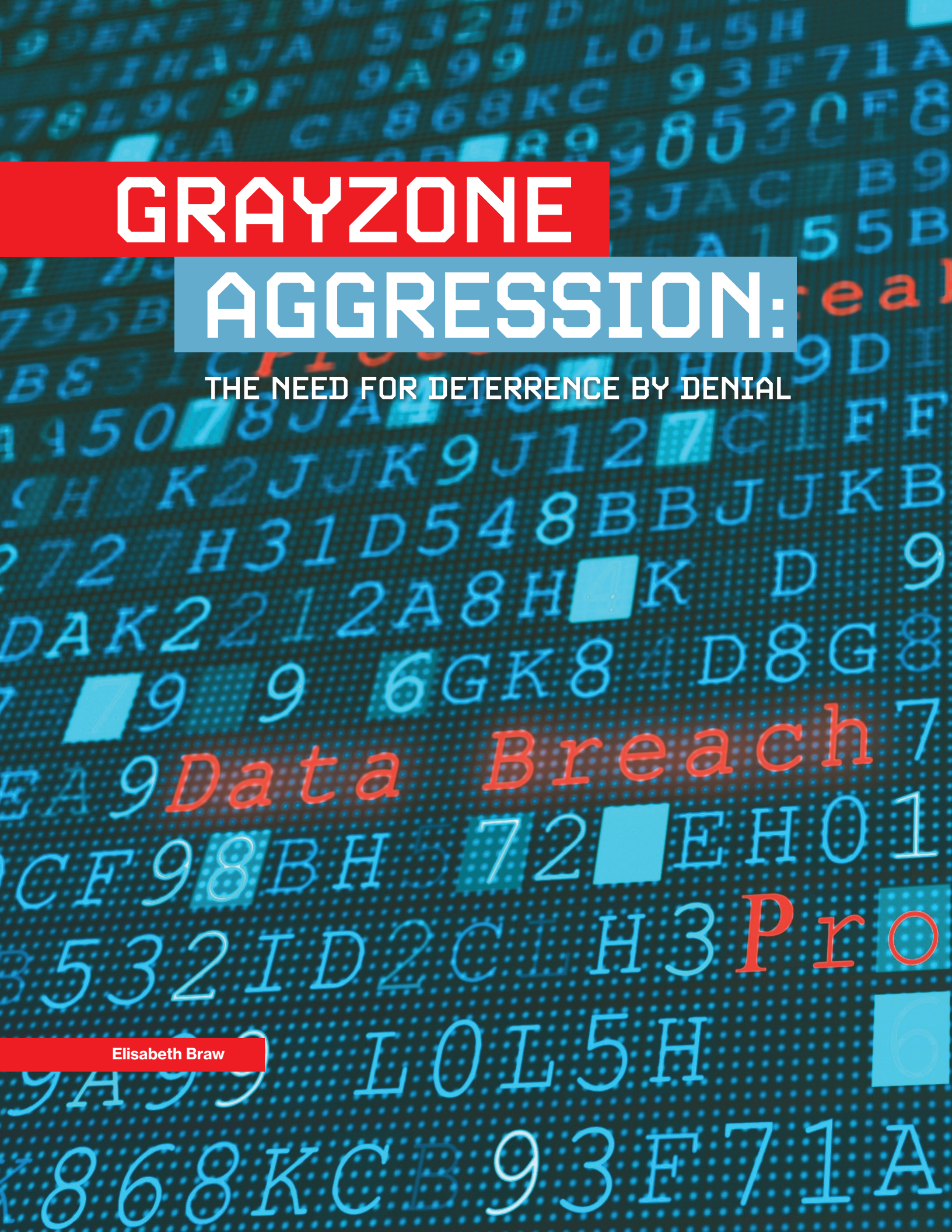

GRAYZONE
AGGRESSION:
THE NEED FOR DETERRENCE BY DENIAL
Data Breach
Pro
Elisabeth Braw

IN MAY 2021, CYBER ATTACKERS ENTERED Colonial Pipeline's system and held the company to ransom. What then ensued was a case study of Western countries' vulnerability to cyber attacks: a fuel shortage ensued, and drivers panicked and stockpiled fuel, which worsened the shortage. Defeating cyber aggression must involve not just strong deterrence-by-punishment signaling but strong deterrence-by-denial signaling too.

When unknown intruders took over parts of Colonial's system on May 6, 2021, executives at the vital pipeline that supplies almost half of all fuel consumed on the East Coast—more than 100 million gallons per day—may have thought they could contain the damage.[1] The following day, however, the intruders presented a ransom demand. Colonial had no choice but to shut down the rest of its system. The attack, though, had been covered by many news outlets, and Colonial's decision to shut the pipeline was covered by even more. Unsurprisingly, drivers on the East Coast concluded that it would become harder to get gasoline and drove to gas stations to fill up, often filling various other containers just in case.[2] Hoarding made sense from an individual perspective, but collectively the drivers dramatically exacerbated the damage caused by the attack. 20% of all Americans, and 30% of people in the affected southeastern states, later said they were personally affected by the attack.[3] Colonial paid the $5 million ransom demanded by the attackers.[4]The attackers, now known to have been the DarkSide group operating in Eastern Europe,[5] could sit back and enjoy both the ransom and the chaos.

The Colonial hack is a case study in the potency of cyber aggression and in how the targeted country can inadvertently contribute to its own misery. Cyber attackers like to target services ordinary citizens need on a daily basis precisely because such attacks cause enormous disruption. A hack on a hospital can cause deaths. A cyber attack against a water company can cause severe illness, as almost happened when a digital intruder entered the water treatment system in Oldsmar, Florida, in February 2021 and raised the water's lye

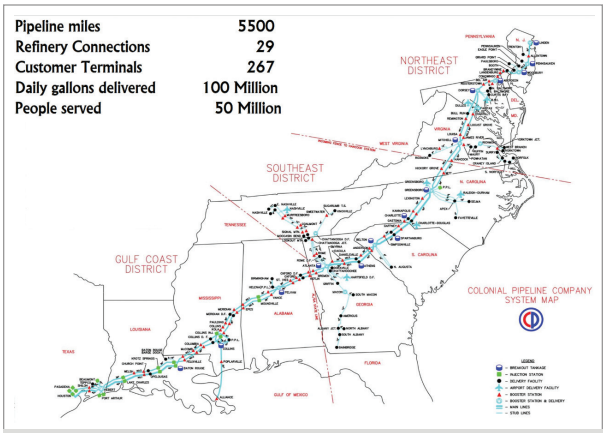
Raleigh, NC United States 05-12-2021: A red plastic bag covers an empty pump at a gas station. Fuel supply to the Southeast was disrupted due to a cyber attack on the Colonial Pipeline. I Sharkshock Adobe Stock

level to 100 times its normal levels.[6] In 2017, the NotPetya attack unleashed by Russia against Ukraine hit at least four hospitals, six power companies, two airports, at least 22 banks, and card payment systems.[7] The virus then traveled to the rest of the world, crippling the Danish shipping giant A. P. Møller Maersk, the US pharmaceutical giant Merck, and a string of other multinationals, saw their operations crippled for days. Several of them sustained losses in the hundreds of millions of dollars.

Cyber attackers like to target services ordinary citizens need because such attacks cause enormous disruption.

At the very least, since the NotPetya incident the US has strengthened its offensive cyber capabilities. The UK and some other NATO allies, too—it is unclear exactly which ones—have offensive cyber. The purpose of offensive cyber is not to randomly attack Western countries' rivals but to strike back if an entity attacks first. That entity may be a hostile state, a group backed by it, or a group acting on its own—though in the latter case, the group can of course be linked to a hostile government without the links being documented in a way that the government of a targeted country can see.

The United States' offensive cyber capabilities, in particular, are thought to be outstanding. As with defense against kinetic aggression, the goal of cyber defense is to demonstrate such force that the attacker decides attacking would not be worth the effort. In the case of traditional, kinetic, military defense, NATO and its member states demonstrate such might through constant exercises. They can do so—indeed, all countries do so—because the prospective attacker's military capabilities are well known. There's no mystery about how one attacks using amphibious forces, special forces, artillery, infantry, and air support. Even armed forces' approximate composition, including weaponry and manpower, is known



Colonial Pipeline System | Sam Whitehead, Public & Government Affairs Manager | CC public domain

to countries' adversaries. That is not the case in the cyber domain, whose weapons, participants, and goals constantly fluctuate, which makes it difficult to conduct exercises that intimidate the adversary. To be sure, cyber forces can demonstrate their capabilities invisibly to the public and visibly to known adversaries. But in doing so, they must demonstrate some of their knowledge about the respective adversary's capabilities—and will prompt the adversary to change tools and tactics. As a result, cyber exercises aimed at signaling to adversaries remain relatively scarce.

Instead, cyber deterrence needs to rely on a combination of deterrence by punishment of select attacks and deterrence by denial. By definition, punishment means that deterrence has failed, but given that it's impossible to deter all cyber attacks and intrusions, Western governments with offensive cyber capabilities could retaliate against specific cyber attackers. The harm done to targets of such retaliation and the arbitrary nature of how they're selected for punishment would increase the cost in most cyber attackers' cost-benefit analysis. The public also expects the government to avenge, particularly egregious cyber attacks: after the Colonial hack, 68% of Americans supported retaliation, while only 12% opposed such action.[8] (It's not known how the US Cyber Command punished DarkSide for the hack.)

As with deterrence of kinetic aggression, deterrence by denial—in effect, deterrence by societal resilience—needs

to join deterrence by punishment. Countries need to demonstrate that even though some cyber attacks will be successful in hitting their target, their effect will be smaller than intended by the perpetrator. Deterrence by denial thus needs to involve the wider public. That means educating the public about what to do if essential services suddenly become unavailable. In 2018, the Swedish Civil Contingencies Agency (MSB) did exactly that with a leaflet called If Crisis or War Comes, which it sent to all households in the country.[9] The leaflet, which has since been followed by similar leaflets in some European countries, contains easy bullet-point instructions for a range of crises, including outages of essential services. In a crisis, some citizens will always panic, but a public prepared for various large contingencies will be able to help reduce the harm.

Four years ago, power at Fort Bragg went off, leaving the base's 50,0 00-some soldiers and officers scrambling to keep operations and daily activities, including food provision going.[10] When the power came back on, the commanders informed the staff that the power outage had been an exercise. Such preparedness helps convince prospective attackers that cyber intrusions are not worth the effort. Companies and communities across Western countries should carry out similar exercises; doing so would not just help them handle disruptions but would also contribute to national deterrence signaling. Together with the signaling of deterrence by punishment, such deterrence by denial will form a combined shield that could reduce, albeit not eliminate, cyber aggression.

Official seal for United States Cyber Command
United States Cyber Command | CC public domain

The goal of cyber defense is to demonstrate such force that the attacker decides attacking would not be worth the effort.

ABOUT THE AUTHOR

Elisabeth Braw is a senior associate fellow at the European Leadership Network, focusing on defence against grayzone and hybrid threats as well as the intersection between geopolitics and the globalised economy. Her book *Goodbye, Globalization: the Return of a Divided World* will be published by Yale University Press in February 2024.

Elisabeth is also a columnist with Foreign Policy and Politico Europe and the author of *The Defender's Dilemma: Identifying and Deterring Grayzone Aggression* (2022). She is a member of GALLOS Technologies' advisory board, a member of the UK National Preparedness Commission, a member of the Krach Institute for Tech Diplomacy's advisory council, and an adviser to Willis Towers Watson's research arm

ENDNOTES

1 Charlie Osborne, "Colonial Pipeline ransomware attack: Everything you need to know," *ZDNET,* May 13, 2021, https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/ (accessed April 18, 2023).

2 Laura Podesta, Jeff Pegues, and Peter Martinez, "Drivers start scrambling for gas as pipeline shutdown continues," *CBS News*, May 12, 2021, https://www.cbsnews.com/news/gas-prices-colonial-pipeline-ransomware-attack/ (accessed April 18, 2023).

3 Kathy Frankovic, "Two-thirds of Americans believe the U.S. should retaliate after Colonial Pipeline cyber attack," *YouGov*, May 20, 2021, https://today.yougov.com/topics/politics/articles-reports/2021/05/20/us-should-retaliate-pipeline-cyberattack (accessed April 18, 2023).

4 Christina Wilkie, "Colonial Pipeline paid $5 million ransom one day after cyberattack, CEO tells Senate," *CNBC*, June 8, 2021, https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html (accessed April 18, 2023).

5 Anthony Freed, "Inside the DarkSide Ransomware Attack on Colonial Pipeline," *Cybereason*, May 10, 2021, https://www.cybereason.com/blog/inside-the-darkside-ransomware-attack-on-colonial-pipeline (accessed April 18, 2023).

6 Jenni Bergal, "Florida Hack Exposes Danger to Water Systems," *The Pew Charitable Trusts*, March 10, 2021, https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/03/10/florida-hack-exposes-danger-to-water-systems (accessed April 18, 2023).

7 Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *WIRED*, August 18, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (accessed April 18, 2023).

8 Frankovic, "Two-thirds of Americans believe the U.S. should retaliate after Colonial Pipeline cyber attack."

9 "The Brochure If Crisis or War Comes," accessed October 25, 2023, https://www.msb.se/en/rad-till-privatpersoner/the-brochure-if-crisis-or-war-comes/.

10 Meghann Myers, "Here's the story behind that massive Fort Bragg power outage," *Army Times*, April 25, 2019, https://www.armytimes.com/news/your-army/2019/04/25/heres-the-story-behind-that-massive-fort-bragg-power-outage/(accessed April 18, 2023).

Wake Forest, NC United States 05-12-2021: A sign is displayed at an empty pump explaining the shortage caused by the Colonial Pipeline cyber attack. Sharkshock | Adobe Stock