"Never Forget": 9/11 Then and Now—Thoughts on Readiness

August 31, 2021 | Dr. Sarah Lohmann

On the morning of September 11, 2001, I stopped by the post office on my way to the newsroom of the Washington, DC–based newspaper where I worked as an editorial writer. I wanted to mail a postcard of the World Trade Center, where I had just been for an interview with a foreign dignitary a few days before.

"This no longer exists," the postal employee said as he looked at the postcard I had shoved into his hand. "Word is, next plane is headed for the Capitol," he said, cranking up the radio.

A few short minutes later, I watched plumes of smoke from the Pentagon clog up the horizon as I drove by on the freeway. Cars were parking on the side of the road, everyone trying to call loved ones. The city was mass pandemonium as Capitol Hill workers abandoned cars and ran, observing the warning the Capitol was to be evacuated.

Finally arriving in the newsroom, I joined shocked colleagues huddled around the television and watching replays of the moment the planes hit the towers. The next week was like one long day. Photographers were sent to get as close to the Pentagon site as possible. Our top journalists were sent to all three sites of the downed planes to do investigative reporting. I was to analyze the events and churn out opinion pieces. With a handful of other big-city newspapers, we were given the Osama bin Laden tape—the one recorded before the attacks in which he talked about his plans for destruction and the angle of impact that causes the most casualties. Horrified, I played it over and over, stopping and starting the tape, jotting down notes, and trying to make sense of it all. For me, the burning Pentagon hurt the most. The Pentagon was more than a familiar landmark that had been part of my backyard since my teen years; it was a symbol of US strength and security.

All week, we kept waiting for the next attack. On the Potomac River in front of my little apartment, warships replaced the little sailboats passing by the small marina across from my home. Tanks and fences surrounded the Capitol. We felt as if we were under siege. And though we did eventually exhale, "We will never forget" became the mantra of every Washington

government agency. This mantra guided key decisions long after the banners scrawled with those words were eventually removed from every bridge in the city. We would soon learn warning signs had presented themselves, but we had not been ready.

While Washington prepared its response, NATO was also clear and purposeful. On the day of the attacks, NATO declared its solidarity with the United States and offered its assistance and support. On September 12, it invoked Article 5 of the North Atlantic Treaty, pending confirmation the attacks had emanated from abroad. The secretary general of NATO, Lord Robertson, invoked Article 5 on October 2 as a result of the conclusions of the international investigation into the attack. Article 5 states an armed attack against one or more allies may be considered an attack against all. These events and that month changed the direction of my career.

Previously focused on human rights in my foreign policy coverage, I was now painfully aware—with the rest of the nation—these could not flourish in a security void. My attention turned to NATO, its expansion, and the terrorist threat to member nations from the Greater Middle East, including Iraq, Afghanistan, and the Mediterranean.[1] I increasingly spent my time traveling to the Eastern European countries that were ready to help support the United States in its fight for democracy and reporting on their progress as they coupled new human rights standards with improved military readiness. Desiring to commit more time to my new interest in the nexus of security and human rights, I left the newspaper a year later to spend the year as a Fulbright scholar researching what NATO's role could be in protecting member nations from terrorist threats in the Greater Middle East.

No longer wanting to stand on the sidelines and record history, but to use my skills for public service, I joined the Civil Service at the Department of State after my Fulbright scholarship ended. Just as the threat to NATO nations in those days was overt and explosive—the 9/11 attacks, the Madrid train bombings of 2004, the London bombings of 2005—so too was the response. Public service in failed states then focused on the tangibles: new schools, new democratic institutions, and expanded voting rights.

The threat to NATO nations remains overt and violent, and member states' response efforts to strengthen civil society in failed states endures. But democracy's enemies today employ weapons initially less visible than those wielded on September 11, 2001.

Cyber war is becoming the tool of choice for nation-states and terrorists as they target critical infrastructure that keeps US families, neighborhoods, and cities safe and healthy. Offensive cybercapabilities are now increasingly being used by nation-states and terrorists alike to target civilians. Twenty years later, another 9/11 is possible, but this time through cyber means.

In the last few months, cyberattacks have impacted US critical infrastructure significantly. The cyberattack on the Colonial Pipeline was the largest such attack in US history.[2] The

resulting fuel shortages caused flights to change schedules, and airports relying on fuel from the pipeline had to scramble to find other suppliers.[3] On May 12, 2021, 71 percent of gas stations in Charlotte ran out of fuel, and the demand for gas had risen 41 percent in five states.[4] By May 14, 88 percent of gas stations in Washington, DC, had run out of fuel.[5] Fuel prices skyrocketed to their highest since 2014 at more than $3 a gallon.[6] Whether the repercussions of the attack were intended, civilians were paying the price.

In their book *Tools and Weapons*, Brad Smith and Carol Anne Browne ask, "Can we wake up the world before a digital 9/11? Or will governments continue to hit the snooze button?"[7]

In May 2017, in the wake of North Korea's "global 'hot' cyberwar" in which the country targeted civilians with the ransomware WannaCry, patients in the United Kingdom were left on operating tables or had their ambulances diverted as a third of Great Britain's National Health Service became paralyzed.[8] Three hundred thousand computers were affected in 150 countries.[9]

More than 230,000 civilians were left without heat and electricity two days before Christmas in Ukraine in 2015 when the energy grid was affectively compromised in a cyberattack, leaving 30 substations off-line.[10] Two years later in July 2017, Russia struck again with NotPetya, using cyberattacks to target electricity firms, banks, government ministries, and newspapers, initially in Ukraine and then in other European nations, the United States, and Australia.[11]

Yet the response by policy makers to whether a cyber 9/11 could occur was often, "No one has been killed. These aren't even attacks on people. They're just machines attacking machines."[12]

The civilians in Ukraine who froze two days before Christmas and the civilians who were left on the operating table in Great Britain may choose to disagree that this form of war is just about machines. Denying how cyber war has impacted, and continues to harm, the lives of civilians is leaving us unprepared.

Closer to home, the FBI and Department of Homeland Security have warned loudly and publicly that the Russians are continuing cyber activities aimed at the US power grid. In these attacks, the Russians intrude into the control rooms of power stations and networks that are supposed to be impenetrable to gain critical information on how industrial control systems are run. The Russians gained access after having planted malware and then sent malware-laden e-mail links to gain remote access to energy networks through third-party contractors. Since 2016, the Russians have been able both to infiltrate the US electrical grid, with a potential future impact still to be recognized, and to penetrate energy and other critical infrastructure systems connected to the nuclear, commercial facilities, water, aviation, and critical manufacturing sectors.[13]

Likewise, the FBI, the National Security Agency, the Cybersecurity & Infrastructure Security Agency, and the United Kingdom's National Cyber Security Centre announced on July 19, 2021,

China's Ministry of State Security had been using criminal hackers to target government and university entities, maritime industries, and naval defense contractors in the United States and Europe to conduct espionage. Tens of thousands of computers worldwide were compromised when the Chinese contractors hacked Microsoft Exchange Server software.[14]

With this much intelligence at US adversaries' fingertips, the United States should not be caught off guard if at some time in the near future, malicious actors trigger a cyber 9/11 that could stop water from flowing, electrical grids from functioning, cell phones from charging, planes from flying, ports from being secure, and nuclear power from being safely stored—whether simultaneously or, more likely, in a staggered, escalating approach at the cost of human life.

The rub is, as was the case 20 years ago, the United States does not lack knowledge of these potential threats. In an increasingly globalized world, the United States has harnessed both intelligence and technology and has the capability to use both to ensure civilian populations are protected. The United States has developed early warning systems, and artificial intelligence and machine learning are helping the nation to adapt to new threats as quickly as they arise. In Greenville, South Carolina, General Electric developed Digital Ghost, technology that successfully found and neutralized a cyberattack in an operating gas turbine at GE Power's manufacturing facility. Digital Ghost combines artificial intelligence and machine learning technologies with sensing and controls to detect, locate, and neutralize cyberattacks.[15]

Yet the United States has taken the patch-and-maintenance approach for critical infrastructure instead of ensuring aging systems are replaced and cybersecurity is included in critical infrastructure and its emerging technology elements from creation to completion. Research on and development of early warning systems and anomaly detection has often been shoved to the bottom of the priority list. For every Digital Ghost being developed, many more sectors and components of critical infrastructure are being left unprotected, creating risk to vast portions of the US civilian population.

The five bipartisan bills passed by the House Committee on Homeland Security in May 2021 to protect critical infrastructure and the supply chain from cyberattacks are a good place to start. The bills would achieve the following.

- H.R. 2980 would allow the Cybersecurity & Infrastructure Security Agency to help critical infrastructure owners mitigate cyberattacks.

- H.R. 3138 would give state and local governments funding to protect their networks against cyberattacks.

- H.R. 3223 would allow the Cybersecurity & Infrastructure Security Agency to conduct regular testing and assessments.

• H.R. 3243 would protect pipelines against cyberattacks.

• H.R. 3264 would provide the Department of Homeland Security with a research and development mandate for supply chain risks.[16]

If the bills are passed in the Senate and implemented, accountability and a focus on long-term resilience rather than short-term fixes must be required.

The question now, as it was 20 years ago, is not what do we know, but what are we going to do about it? Remembering is the job of every citizen impacted on September 11, 2001. Waking the world before a cyber 9/11 will be a daunting task. But every time we secure innovation and prepare our populations to protect the resources and critical infrastructures they need to survive, we show we will never forget.

ENDNOTES

---

[1] Sarah Means Lohmann, "NATO, Iraq and the German-American Waltz," *National Interest*, January 15, 2003, https://nationalinterest.org/article/nato-iraq-and-the-german-american-waltz-2225; Chuck Hagel, "The United States, NATO, and the Greater Middle East" (speech, US Mission to NATO, Brussels, January 23, 2004), https://www.kas.de/documents/252038/253252/7_dokument_dok_pdf_3929_2.pdf/1c84cfde-3f72-e5df-a50c-c64fdc3b4fbf?version=1.0&t=1539667069095; and R. Nicholas Burns, "The New NATO and the Greater Middle East" (speech, Conference on NATO and the Greater Middle East, Prague, October 19, 2003), https://2001-2009.state.gov/p/eur/rls/rm/2003/25602.htm.

[2] Gloria Gonzalez, Ben Lefebvre, and Eric Geller, " 'Jugular' of U.S. Fuel Pipeline System Shuts Down after Cyberattack," Politico, May 8, 2021, https://www.politico.com/news/2021/05/08/colonial-pipeline-cyber-attack-485984.

[3] Tracy Rucinski, "American Airlines Adds Stops to Two Flights after Pipeline Outage," Reuters, May 10, 2021, https://www.reuters.com/business/energy/american-airlines-adds-fuel-stops-two-flights-after-pipeline-outage-2021-05-11/; and Leslie Josephs, "Pipeline Outage Forces American Airlines to Add Stops to Some Long-Haul Flights, Southwest Flies in Fuel," CNBC, May 10, 2021, https://www.cnbc.com/2021/05/10/colonial-pipeline-shutdown-forces-airlines-to-consider-other-ways-to-get-fuel.html.

[4] Ron Lee, "GasBuddy Reports 71% of Gas Stations without Fuel in Charlotte Metro amid Colonial Pipeline Shutdown," WBTV, May 12, 2021, https://www.wbtv.com/2021/05/11/long-lines-charlotte-gas-supply-squeezed/; and Rachel Frazin and Zack Budryk, "Gas Shortages

Spread to More States," The Hill, May 12, 2021, https://thehill.com/policy/energy-environment/553192-gas-shortages-spread-to-more-states.

[5] Emily Crane, "Gas Runs Out in Joe's Backyard: 88% of DC's Gas Stations Are Empty as Fuel Price Climbs to $3.04 a Gallon after Colonial Pipeline Reopens: Russian Hackers DarkSide 'Shut Down' after Getting $5M Ransom," *Daily Mail*, updated May 15, 2021, https://www.dailymail.co.uk/news/article-9579325/U-S-capital-running-gas-Colonial-Pipeline-recovers.html.

[6] Will Englund and Ellen Nakashima, "Panic Buying Strikes Southeastern United States as Shuttered Pipeline Resumes Operations," *Washington Post*, May 12, 2021, https://www.washingtonpost.com/business/2021/05/12/gas-shortage-colonial-pipeline-live-updates/.

[7] Brad Smith and Carol Ann Browne, *Tools and Weapons: The Promise and the Peril of the Digital Age* (New York: Penguin Random House, 2021).

[8] Smith and Browne, *Tools and Weapons*, 67–69.

[9] Smith and Browne, *Tools and Weapons*, 67–69.

[10] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[11] Pavel Polityuk and Alessandra Prentice, "Ukrainian Banks, Electricity Firm Hit by Fresh Cyber Attack," Reuters, June 27, 2017, https://www.reuters.com/article/us-ukraine-cyber-attacks-idUSKBN19I1IJ; and Nicole Perlroth, Mark Scott, and Sheera Frenkel, "Cyberattack Hits Ukraine Then Spreads Internationally," *New York Times*, June 27, 2017, https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html.

[12] Smith and Browne, *Tools and Weapons*, 71.

[13] Nicole Lindsey, "Russia and China Can Cripple Critical Infrastructure in the United States," CPO Magazine, February 12, 2019, https://www.cpomagazine.com/cyber-security/russia-and-china-can-cripple-critical-infrastructure-in-united-states/; Rebecca Smith and Rob Barry, "America's Electric Grid Has a Vulnerable Back Door—and Russia Walked through It," *Wall Street Journal*, January 10, 2019, https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112; and "Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," Cybersecurity & Infrastructure Security Agency, March 15, 2018, https://us-cert.cisa.gov/ncas/alerts/TA18-074A.

[14] Eric Tucker, "Microsoft Exchange Hack Caused by China, US and Allies Say," Yahoo News, July 19, 2021, https://news.yahoo.com/microsoft-exchange-email-hack-caused-110149294.html?guccounter=1.

[15] "Digital Ghost: Real-Time, Active Cyber Defense," General Electric, n.d., https://www.ge.com/research/offering/digital-ghost-real-time-active-cyber-defense.

[16] Sergiu Gatlan, "US Introduces Bills to Secure Critical Infrastructure from Cyber Attacks," Bleeping Computer, May 19, 2021, https://www.bleepingcomputer.com/news/security/us-introduces-bills-to-secure-critical-infrastructure-from-cyber-attacks/.

*****