Published on *American Council on Science and Health* (https://www.acsh.org)

Cyberattacks as a Public Health Threat

By Alex Berezow, PhD — October 28, 2020

The first known death from a cyberattack raises the prospect that malware could be more than just a financial crime.

Credit: Batorry / Wikipedia [1]

This article was originally published at Geopolitical Futures. The original is here [2].

Traditionally, military, government and financial institutions have been the primary targets of international cyberattacks. But the COVID-19 pandemic has revealed the extent to which soft targets such as pharmaceutical companies and hospitals are attractive. It’s time to consider the geopolitical reality that cyberattacks can threaten public health and safety.

Coming to a Hospital Near You

Before the coronavirus pandemic, there were minimal consequences to a cyberattack on public health targets. The tampering with pharmaceuticals or the death of patients in a hospital would make medical institutions and governments look weak or negligent, but the domestic and geopolitical impact would have been minimal. But the pandemic has put public health at the center of national concern and has pitted political and health institutions against one another. As a result, deep political and social tensions have been exposed. This now makes attacking public health more attractive because the consequences of doing so would yield higher returns. Now, an attack on public health could cause real problems for governments – by creating, for example, a social backlash that threatens stability or diverts attention and resources elsewhere.

Until now, attacks on public health targets focused primarily on financial returns for the attacker.

Indeed, a recent attack was directed at eResearchTechnology [3], a company that provides software to other companies that perform clinical trials, including ones testing treatments for coronavirus. The type of attack used by the hackers is known as ransomware, malicious software that blocks the ability of an organization to access its own data. The term “ransomware” comes from what follows next: The target will be allowed to access its data only after it pays a ransom to the perpetrators. Most victims tend to pay off the hackers rather than hire a team of experts to get their data back. This is partly due to the cost of the experts, partly to the target’s embarrassment, partly to insurance companies that offer cyberattack coverage [4], and partly to the increasing sophistication of cybercriminals who use advanced cryptographic methods [5] that make it nearly impossible to recover the data without a secret key. As a result, ransomware attacks are an increasingly common form of extortion.

In the case of eResearchTechnology, clinical trials were slightly delayed, but it appears that disaster was largely avoided. That’s not always the case. In September, hackers – likely from Russia – conducted a ransomware cyberattack on University Hospital Dusseldorf in Germany [6], causing a disconnection between the hospital and ambulance computer networks. A woman with a life-threatening condition could not be admitted and was driven to a different hospital farther away. Due to the delay in treatment, she died, becoming the first known death due to a cyberattack.

Other examples abound. A ransomware attack crippled the city of Baltimore for months [7], causing service delays and a temporary shutdown of its emergency dispatch system. The Champaign-Urbana Public Health District in Illinois was hit by a ransomware attack [8] that prevented the organization from communicating to the public about COVID-19. In 2019, at least 759 ransomware attacks occurred on health care providers in the U.S. [9] Cybercriminals even exploited the COVID-19 pandemic, sending fake emails to hospitals promising items such as N95 masks or ventilators, as a way to infect computers with malicious software. It’s little surprise, then, that in a sobering analysis of the ransomware threat facing the health care industry [10], the American Hospital Association noted that a ransomware attack is not simply a financial crime; it is a threat-to-life crime because it prevents hospitals from treating patients.

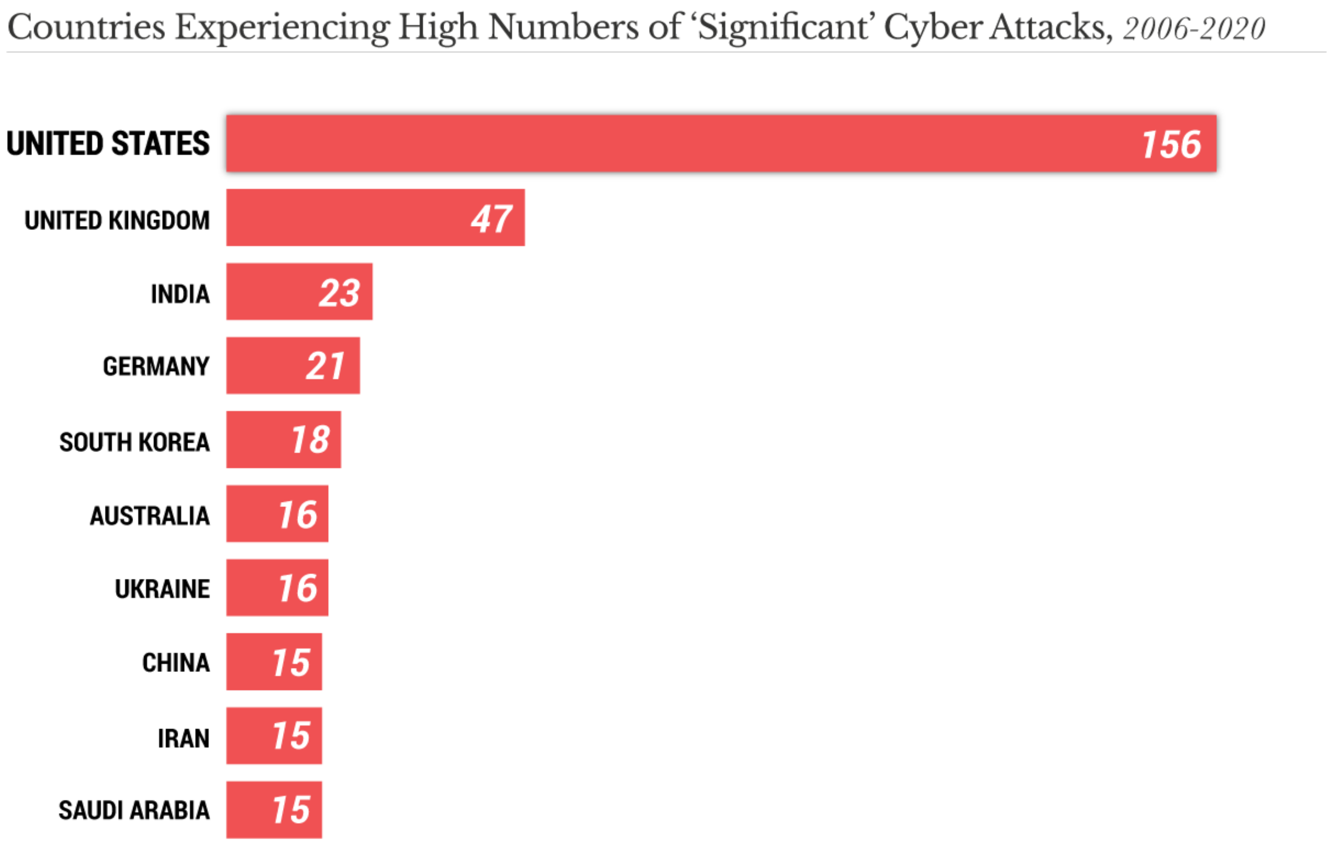
The health care industry and public health institutions are poorly equipped to deal with cyberattacks. Public health has never really been considered a national security interest and therefore does not have a lot of security in place or coordination with the government compared to other high-value cyberattack targets. Health care providers (understandably) lack the expertise and resources needed to prevent cyberattacks [11].

Unfortunately, there is no magic bullet to prevent a cyberattack. The official U.S. government advice given to companies [12] isn’t all that different from what the average internet user is told: update software, use secured internet connections, implement email filters, don’t click on suspicious links or files, and definitely don’t respond to that friendly Nigerian prince. The latter lesson is something the state of Washington learned recently after a Nigerian fraud ring stole roughly $650 million in COVID-19-related unemployment benefits [13]. But that was just money. A cyberattack that targeted Seattle area hospitals during the peak of the coronavirus pandemic could have been lethal.

To be clear, ransomware isn’t the only kind of cyberattack. Each has its own purpose: to make money, to disrupt or sabotage, or to gather intelligence. And though public health institutions have generally been targeted with the former in mind, they could well be targeted with the latter two in mind, especially since it could incite panic among the public or delay potential vaccines.

The Geopolitics of Cyberattacks

Unsurprisingly, the United States is the world's primary target for major cyberattacks, defined by the Center for Strategic and International Studies as "cyberattacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars." The company Specops Software analyzed the data [14] and found that the U.S. was hit by 156 such attacks between May 2006 and June 2020. The U.K. (47 attacks), India (23), Germany (21) and South Korea (18) rounded out the top five. The report notes that most attacks are either distributed denial-of-service (which overwhelm websites with fake traffic) or meant to acquire sensitive information.



Note: 'Significant' cyber attacks include any cyber attacks on a country's government agencies, defense and high tech companies, or economic crimes equating to a loss of more than a million dollars

Source: SpecOps

Graphic redesign by Geopolitical Futures

The top four perpetrators of cyberattacks are China, Russia, Iran and North Korea [15]. However, major cyberattacks are increasingly performed by organized crime groups. Complicating the geopolitical landscape is that many of these attacks are also state-sponsored. A hostile government may want to conduct a cyberattack for a variety of reasons, with sabotage (e.g., the Stuxnet worm that Israel and the U.S. developed to target Iranian nuclear facilities) or intelligence gathering probably the most likely. But as the coronavirus has shown, undermining a nation's ability to respond to infectious disease outbreaks or other natural disasters may allow some countries to achieve geopolitical objectives.

Because cyberattacks are expected to rise as the number of targets increases, prevention seems nearly impossible. It could be, therefore, that the best defense is a good offense. A similar concept could help reduce cyberattacks, but it certainly would not eliminate them for at least three reasons. First, cyberattacks are difficult to trace, and any state sponsor would have plausible deniability. Second, cyberattacks can be perpetrated by organized crime groups or rogue actors, and there may be little that some governments can do to stop them. And third, cybercriminals are always a few steps ahead of law enforcement. As the cyberweapons become more sophisticated, the threat to public health increases.

Source URL: https://www.acsh.org/news/2020/10/28/cyberattacks-public-health-threat-15113

Links

[1] https://en.wikipedia.org/wiki/Laptop#/media/File:Samsung_QX-511_(2).JPG
[2] https://geopoliticalfutures.com/cyberattacks-as-a-public-health-threat/
[3] https://www.nytimes.com/2020/10/03/technology/clinical-trials-ransomware-attack-drugmakers.html
[4] https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks
[5] https://www.crn.com/news/channel-programs/tyler-technologies-reportedly-paid-ransomware-like-many-other-victims-expert-says
[6] https://www.thelocal.de/20200922/german-experts-see-russian-link-in-deadly-hospital-hacking
[7] https://www.baltimoresun.com/news/crime/bs-md-ci-hack-folo-20180328-story.html
[8] https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2020/04/13/hospital-hackers-seize-upon-coronavirus-pandemic
[9] https://www.pcmag.com/news/2019-the-year-ransomware-feasted-on-the-us-public-sector
[10] https://www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed
[11] https://www.theverge.com/2019/4/4/18293817/cybersecurity-hospitals-health-care-scan-simulation
[12] https://www.nist.gov/blogs/manufacturing-innovation-blog/how-protect-your-business-cyber-attacks
[13] https://www.washingtonpolicy.org/publications/detail/the-employment-security-department-fraud-tops-650-million-and-will-grow-higher
[14] https://specopssoft.com/blog/countries-experiencing-significant-cyber-attacks/
[15] https://www.usnews.com/news/best-countries/articles/2019-02-01/china-and-russia-biggest-cyber-offenders-since-2006-report-shows