Cyberattacks on Infrastructure in the United States

Cyberattacks on critical infrastructure have increasingly become a major concern for national security. The **Colonial Pipeline ransomware attack** in May 2021, carried out by the Russian-linked group DarkSide, disrupted fuel supplies across the East Coast for **six days** and caused panic buying of gasoline. The attack cost the company **$4.4 million in ransom**, though only part of it was recovered, and it is considered one of the most destructive cyberattacks on U.S. energy infrastructure to date (Reuters, 2025a). No deaths were reported, but the economic disruption was widespread, highlighting vulnerabilities in energy systems.

Similarly, the **Stuxnet worm** of 2010, a sophisticated cyber weapon likely developed by the United States and Israel, targeted Iran's nuclear facilities and set a precedent for industrial sabotage. While not directly targeting U.S. systems, it underscored the potential for cyberattacks to disrupt critical infrastructure globally (Politico, 2024).

In the **2017 WannaCry ransomware attack**, hospitals across the globe, including some in the U.S., were paralyzed. Medical devices were rendered unusable, and surgeries were postponed, demonstrating the risk to healthcare systems. British hospitals reported **deaths from delayed care**, though the exact numbers remain uncertain (Food and Wine, 2025). In the U.S., flights were also grounded during various cyber incidents, such as a ransomware attack in 2021 that affected the IT systems of the Federal Aviation Administration (FAA) (Reuters, 2025a).

Water and wastewater systems are also at significant risk. The Environmental Protection Agency found that water systems serving **193 million people** are vulnerable to cyberattacks. Such incidents could result in the contamination or shutdown of drinking water supplies (Food and Wine, 2025).

The U.S. government has responded with initiatives such as the **Cybersecurity and Infrastructure Security Agency (CISA)** and the **National Cybersecurity Strategy**, which emphasize mandatory reporting of cyber incidents and public-private collaboration to bolster defenses (Rand Corporation, 2024).

Cyberattacks on Infrastructure in Maryland

Maryland, with its proximity to Washington, D.C., and concentration of federal agencies, remains a prominent target for cyberattacks. The **2019 Baltimore ransomware attack**, executed by a group called RobbinHood, lasted **over two weeks**, locking city systems and preventing access to email and payment portals. The city refused to pay the **$76,000 ransom** but spent **$18 million** on recovery and rebuilding IT infrastructure (Politico, 2024). No deaths occurred, but critical city services were severely disrupted. Baltimore County Public Schools suffered a ransomware attack in 2020 during the COVID-19 pandemic, which disrupted online learning for **115,000 students** for nearly a week. The attack highlighted the vulnerabilities of educational systems during a critical time for remote learning (ODNI, 2024).

Healthcare systems in Maryland are also frequent targets. Hospitals within the University of Maryland Medical System have faced ransomware attacks that **temporarily shut down critical IT systems**,

delaying care and increasing risks to patients during high-demand periods (Maryland Attorney General, 2024).

Maryland's **Maryland Cybersecurity Council** has spearheaded efforts to strengthen the state's defenses, including mandating stronger cybersecurity practices for state agencies. Additionally, the Maryland Air National Guard's **Cyber Fortress 3.0** training exercise tested responses to potential attacks on power grids and water systems (National Guard, 2024).

The University of Maryland's START program has been instrumental in developing a dataset on cyberattacks targeting critical infrastructure, offering insights into regional and national trends. These efforts are supported by **$6.5 million in state and federal funding** aimed at bolstering local cybersecurity capabilities (Raskin House, 2024).

CrowdStrike's Role in Cybersecurity and Addressing Cyberattacks

CrowdStrike, a leading cybersecurity company founded in 2011, has played a pivotal role in identifying and mitigating cyber threats against critical infrastructure in the United States and globally. CrowdStrike is best known for its **Falcon platform**, which provides AI-driven, cloud-native endpoint protection and advanced threat intelligence.

Key Incidents and CrowdStrike's Role

1. Democratic National Committee (DNC) Hack (2016):
    - CrowdStrike was instrumental in attributing this hack to two Russian state-backed groups, Cozy Bear and Fancy Bear, linked to the Russian intelligence agencies (Reuters, 2025a).
    - The hack persisted over several months before detection.
    - The attack exposed sensitive emails and influenced political narratives during the U.S. presidential election.
    - The fallout included reputational damage and financial costs associated with improved cybersecurity measures.
    - No deaths occurred, but the incident emphasized the potential for cyberattacks to disrupt democratic processes.
2. Healthcare and Hospital Attacks:
    - CrowdStrike has been involved in addressing ransomware attacks on healthcare systems, including the WannaCry attack in 2017, which disrupted hospital operations globally.
    - Medical devices were rendered inoperable, critical surgeries were delayed, and some treatment interruptions were linked to patient deaths (Food and Wine, 2025).
    - The global cost of WannaCry exceeded $4 billion.
3. Colonial Pipeline Attack (2021):
    - CrowdStrike contributed to understanding the tactics of the DarkSide group, a ransomware collective responsible for the attack.
    - The attack lasted six days, causing fuel shortages across the East Coast.
    - Colonial Pipeline paid $4.4 million in ransom, although some of it was recovered later (Reuters, 2025a).

    - No direct fatalities were reported, but the incident highlighted the risks of delayed emergency responses due to fuel shortages.
4. Microsoft Outage and Air Travel Delays (2023):
    - While CrowdStrike did not directly attribute the cause of the outage, it investigated disruptions stemming from vulnerabilities in cloud-based systems.
    - The outage disrupted critical systems for several hours globally.
    - More than 3,500 flights were delayed, and airline communication systems were temporarily disabled (NBC Washington, 2023).
    - Banks, airlines, and global companies faced service disruptions, highlighting the cascading effects of cloud-based system vulnerabilities.
5. Aviation and Transportation Attacks:
    - CrowdStrike has monitored and mitigated cyber threats against aviation systems, such as ransomware attacks on the FAA in 2021 that grounded dozens of flights.
    - These incidents caused economic losses and logistical challenges for airlines and passengers (Reuters, 2025a).

Broader Impact of CrowdStrike on Cybersecurity

- Detection and Response:
    - CrowdStrike's Falcon OverWatch continuously monitors and detects threats in real time, providing rapid response to mitigate damages.
    - The platform uses behavioral analytics and AI to identify potential attacks before they escalate.
- Cost Savings and Prevention:
    - Organizations leveraging CrowdStrike's services often avoid the multimillion-dollar costs associated with ransomware payments and operational downtime.
    - CrowdStrike assists companies in avoiding indirect costs such as legal fees, reputational damage, and customer attrition.
- Public-Private Collaboration:
    - CrowdStrike collaborates with government agencies, including the FBI and Department of Homeland Security (DHS), to share intelligence on cyber threats.
    - The company has participated in national efforts to safeguard elections, critical infrastructure, and corporate assets.
- Impact on Maryland:
    - Given Maryland's role as a cybersecurity hub, CrowdStrike engages with institutions like the NSA, Cyber Command, and regional entities to bolster local cyber defenses.
    - The company contributes to cybersecurity workforce development through partnerships with academic institutions such as the University of Maryland.

References

1. NBC Washington. (2023). Microsoft Outage Disrupts Flights, Banks, Companies Globally. Retrieved from https://www.nbcwashington.com
2. Food and Wine. (2025). EPA Finds the Drinking Water for 193 Million People in the U.S. Is Vulnerable to Cyberattacks. Retrieved from https://www.foodandwine.com
3. Maryland Attorney General. (2024). Maryland Cybersecurity Council Interim Report. Retrieved from https://www.marylandattorneygeneral.gov
4. National Guard. (2024). Maryland Airmen Test Cyber Skills in Virginia Exercise. Retrieved from https://www.nationalguard.mil
5. ODNI. (2024). Recent Cyber Attacks on U.S. Infrastructure. Retrieved from https://www.dni.gov
6. Politico. (2024). U.S. Allies Accuse Russia of Cyberattacks. Retrieved from https://www.politico.com
7. Rand Corporation. (2024). Threats to America's Critical Infrastructure. Retrieved from https://www.rand.org
8. Raskin House. (2024). Maryland Delegation Announces Funding to Enhance Cybersecurity. Retrieved from https://raskin.house.gov
9. Reuters. (2025a). As China Hacking Threat Builds, Biden to Order Tougher Cybersecurity Standards. Retrieved from https://www.reuters.com
10. Reuters. (2025b). U.S. Has Responded to Chinese-Linked Cyberattacks. Retrieved from https://www.reuters.com
11. START. (2024). Dataset on Cyberattacks Against Critical Infrastructure. Retrieved from https://www.start.umd.edu