Risk of New York City's Electric Power Networks Against Compound Extreme Floodings and Cyberattacks

Charalampos C. Avraam
Postdoctoral Associate, Center for Urban Science and Progress, New York University, Brooklyn, NY, USA

Yury Dvorkin
Associate Research Professor, Dept. of Electrical and Computer Engineering, Dept. of Civil and Systems Engineering, Ralph O'Connor Sustainable Energy Institute, Johns Hopkins University, Baltimore, MD, USA

Luis Ceferino
Assistant Professor, Center for Urban Science and Progress and Dept. of Civil and Urban Engineering, New York University, Brooklyn, NY, USA

ABSTRACT:
The growing frequency of extreme weather events and cyberattacks triggers the rise of compound cyber-physical threats where a cyberattacker targets critically stressed electricity generators and transmission lines during an extreme weather event. In this paper, we quantify the conditional probability of a cyberattack against electric power network components in the event of extreme flooding in the Manhattan Borough of New York City (NYC). Based on the first stage of a recently-proposed framework, a bilevel optimization problem represents the adversarial rationale of a cyberattacker. Our results reveal the risk profiles of electricity generators, transmission lines, and customers in Manhattan, by exploring the parameter space of the bilevel optimization problem through Monte Carlo simulations. We found that when imports from neighboring states are constrained under extreme flooding, the cyberattacker targets natural gas capacity in the NYC Metropolitan Area first, and then transmission lines connecting Manhattan to the NYC Metropolitan Area. The disruption can lead to power outages for more than 50% of Midtown Manhattan customers with high probability. Our analysis informs the design of mitigation and response strategies against compound extreme floodings and cyberattacks.

1. Introduction

Extreme weather events and cyberattacks increase in frequency and compromise the supply of electricity for extended time periods. Data breaches in the U.S. increased by more than 1000% between 2005 and 2022 (Statista, 2021), while the annual 10-year average frequency of extreme weather events in the U.S. grew by more than 400% between 1980-1989 and 2010-2019 (Smith, 2021). The flooded substation in the East 14th street of Manhattan, New York City (NYC) during Hurricane Sandy in 2012 left almost 2 million customers without power (NYC, 2013). The winter storm and associated floodings in Los Angeles, CA left 145,000 customers without power in January 2023 (Mendoza, 2023).

Contrary to the randomness of extreme weather events, cyberattacks are deliberate. A cyberattacker chooses which components to compromise based on their vulnerability and the goal of the cyberattack. When an infrastructure operates under critical conditions, a cyberattack can further exacerbate the impact (Avraam et al., 2022). Hence, an extreme weather event is an opportunity for the cyberattacker to maximize infrastructure damage and exacerbate service disruptions. The imminent threat has alerted U.S. federal and state agencies. For example, on September 14, 2018, North Carolina State officials warned residents against cyberattacks in the onset and immediate aftermath of Hurricane Florence (NCDIT, 2018).

Existing risk frameworks omit the compounding effect of a deliberate cyberattack during an extreme weather event. Risk assessment of compound threats is limited to compound natural hazards (Zscheischler et al., 2018). When studied together, cyberattacks are treated similarly to extreme weather events for the design of preparedness and mitigation strategies (Ouyang, 2017), and information recovery (Soltan et al., 2018). Contrary to extreme weather events, cyberattacks are deliberate and can target critically-stressed infrastructure components to exacerbate the impact of the event. However, frameworks that identify the adversarial rationale of a cyberattacker focus on identifying vulnerable infrastructure components and sectors of the economy (Avraam et al., 2022) and do not provide a cyber-risk profile of individual components.

The increasing frequency of high-intensity hurricanes exposes large coastal cities, *e.g.,* NYC and Los Angeles, to severe floodings (Sanders et al., 2023). Over 50% of electricity generation capacity in the NYC Metropolitan Area was within the 1-percent annual chance floodplain in 2019 (NYCEM, 2019). In this paper, we focus on Manhattan, as the most densely-populated region of the U.S. (USCB, 2021). Given our limited knowledge on cyberattacker capabilities, in this paper we investigate:

- What is the conditional probability of a cyberattack in the event of extreme flooding in Manhattan?
- What is the risk profile of customers, electricity generators, and transmission lines of the Manhattan electric power network?

The rest of the paper is organized as follows. Section 2 describes the probabilistic framework in this paper, which explores the parameter space of the cyberattacker bilevel optimization problem in Avraam et al. (2022). In Section 3, we detail the assumptions of our scenario design. We discuss results and limitations in Section 4, and conclude in Section 5.

2. Methods

For completeness, we first summarize the optimization problems of the system operator and cyberattacker, as in Avraam et al. (2022). Then, we describe the assumptions of the probabilistic analysis for the electric power components of Manhattan. Figure 1 illustrates the methodology in this paper.

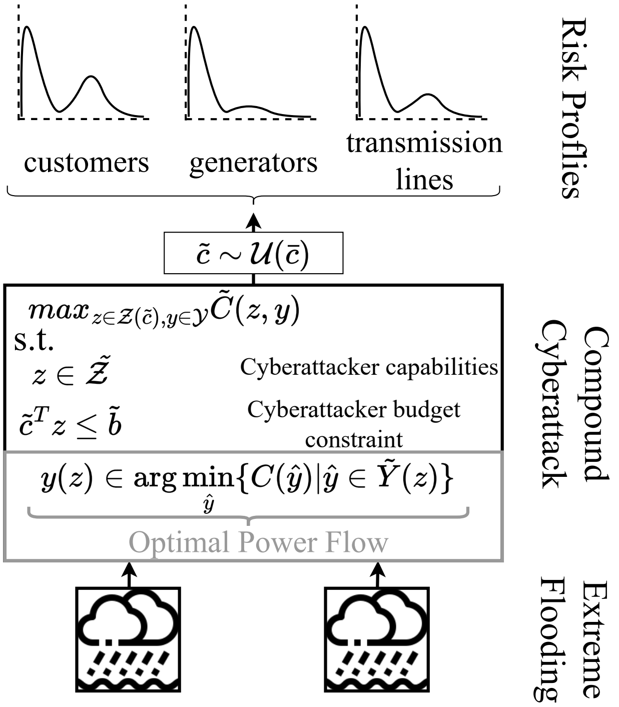
customers
generators
transmission lines
Risk Proflies
$\tilde{c} \sim \mathcal{U}(\bar{c})$
$max_{z\in\mathcal{Z}(\tilde{c}),y\in\mathcal{Y}}\tilde{C}(z,y)$
s.t.
$z \in \tilde{\mathcal{Z}}$
Cyberattacker capabilities
$\tilde{c}^T z \leq \tilde{b}$
Cyberattacker budget constraint
$\underbrace{y(z) \in \arg\min_{\hat{y}}\{C(\hat{y})|\hat{y} \in \tilde{Y}(z)\}}_{\text{Optimal Power Flow}}$
Compound Cyberattack
Extreme Flooding

Figure 1: Probabilistic framework for the generation of cyber risk profiles of electricity customers and components under extreme flooding and uniform distribution of the vulnerability of electric power components to cyberattacks.

2.1. System Operator: Optimal Power Flow Model

Following Avraam et al. (2022), we model the electricity infrastructure as a network where $\mathscr{N} = \{1,\ldots,N\}$, $\mathscr{E} = \{1,\ldots E\}$ and $\mathscr{G} = \{1,\ldots G\}$ are the sets of nodes, edges, and electricity generation technologies in the network, with $N,E,G \in \mathbb{N}$.

Agents in the network make decisions in hourly intervals $h \in \mathscr{H}$ for a representative day of the Fall hurricane season. The system operator in our framework minimizes the operating cost based on the cost of electricity generation ($c^g_h \in \mathbb{R}^{N\times G}$) and the cost of unserved load ($c^u_h \in \mathbb{R}^N$):

$$C(g,u) = \sum_{h\in\mathscr{H}} \left(c^g_h\right)^T g_h + \sum_{h\in\mathscr{H}} \left(c^u_h\right)^T u_h, \qquad (1)$$

to decide the dispatching of electricity generation technologies ($g_h \in \mathbb{R}^{N\times G}$), unserved load ($u_h \in \mathbb{R}^N$), power flow across edges ($f_h \in \mathbb{R}^E$) and nodal voltage angle ($\theta \in \mathbb{R}^N$). In addition, the system operator needs to satisfy electricity generation and flow constraints. The optimization problem of the system operator in Eq. (2) is an Optimal Power Flow (OPF) model (Eldridge et al., 2018).

$$\min_{\substack{g_h \in \mathbb{R}^G, f_h \in \mathbb{R}^E,\\ u_h, \theta_h \in \mathbb{R}^N}} \quad C(g,u)$$

$$\begin{aligned}
&\text{s.t.} && && (2a)\\
&\begin{matrix}\sum_{i\in\mathscr{G}} g_{ih} + u_h \\ -d_h + A^T f_h = 0\end{matrix}, && \forall h \in \mathscr{H} && (2b)\\
&f_h + BA\theta_h = 0, && h \in \mathscr{H} && (2c)\\
&\underline{g}_h \le g_h \le \bar{g}_h, && \forall h \in \mathscr{H} && (2d)\\
&\underline{f}_h \le f_h \le \bar{f}_h, && \forall h \in \mathscr{H} && (2e)\\
&\underline{\theta}_h \le A\theta_h \le \bar{\theta}_h, && \forall h \in \mathscr{H} && (2f)\\
&0 \le u_h \le d_h, && \forall h \in \mathscr{H} && (2g)\\
&\theta^{ref}_h = 0, && \forall h \in \mathscr{H} && (2h)
\end{aligned}$$

In our formulation, Eq. (2b) ensures that demand for electricity ($d_h \in \mathbb{R}^N$) is met at all nodes of the network, where $A \in M_{E\times N}(\mathbb{R})$ is the incidence matrix of the electric power network. Moreover, Eq. (2c) ensures that nodal voltage angles are consistent with the flow of electricity between nodes, where $B = \text{diag}\{b\} \in M_{E\times E}(\mathbb{R})$ is the matrix of susceptances of all transmission lines. In addition, Eqs. (2d)-(2g) describe the upper and lower bounds on generation ($\bar{g}_h, \underline{g}_h \in \mathbb{R}^{N\times G}$), flow across transmission lines ($\bar{f}_h, \underline{f}_h \in \mathbb{R}^E$), and nodal voltage angle differences across edges ($\bar{\theta}_h, \underline{\theta}_h \in \mathbb{R}^E$) respectively. Finally, Eq. (2h) defines the reference node, *i.e.,* the node whose voltage angle (θ^{ref}_h) serves as a reference for the level of all other voltage angles.

2.2. *Cyberattacker: Bilevel Optimization Problem*

Similarly to Avraam et al. (2022), the cyberattacker can compromise generation capacity ($z^g_{sh} \in \mathbb{R}^{N\times G}$), flow capacity ($z^f_{sh} \in \mathbb{R}^E$), and tamper with nodal voltage angle measurements ($z^\theta_{sh} \in \mathbb{R}^N$). The vector $(z^g_{sh}, z^f_{sh}, z^\theta_{sh}) \in \mathbb{R}^{N\times G} \times \mathbb{R}^E \times \mathbb{R}^N$ defines the *cyberattacker strategy* and reveals the targeted components. The cyberattacker strategy implies that Eqs. (2d)-(2g) of the OPF (2) become:

$$\begin{aligned}
\underline{g}_h \quad &\le g_h \quad \le \bar{g}_h - z^g_h, \quad && h \in \mathscr{H} && (3a)\\
\underline{f}_h - z^f_h &\le f_h \quad \le \bar{f}_h - z^f_h, && h \in \mathscr{H} && (3b)\\
\underline{\theta}_h - z^\theta_h &\le A\theta_h \le \bar{\theta}_h - z^\theta_h, && h \in \mathscr{H} && (3c)
\end{aligned}$$

The cyberattacker decides the strategy that maximizes the total unserved load across nodes of the electric power network, *i.e.,*

$$\max_{\substack{z^g_h \in \mathbb{R}^G, z^f_h \in \mathbb{R}^E,\\ z^\theta_h \in \mathbb{R}^E, y \in \mathscr{Y}}} \quad \sum_{h\in\mathscr{H}} \mathbf{1}^T_N u_h$$

$$\begin{aligned}
&\text{s.t.} && (4a)\\
&y \in \arg\min_{\hat{y}} \left\{ C(\hat{y}; z^g, z^f, z^\theta) \;\middle|\; \begin{matrix}(2b)-(2c),\\ (3a)-(3c),\\ (2g)-(2h)\end{matrix} \right\} && (4b)\\
&0 \le z^g_h \le \bar{g}_h, \quad \forall h \in \mathscr{H} && (4c)\\
&0 \le z^f_h \le \bar{f}_h, \quad \forall h \in \mathscr{H} && (4d)\\
&0 \le z^\theta_h \le \bar{\theta}_h, \quad \forall h \in \mathscr{H} && (4e)\\
&\sum_{h\in\mathscr{H}} \left(\tilde{c}^g_h\right)^T z^g_h + \left(\tilde{c}^f_h\right)^T z^f_h + \left(\tilde{c}^\theta_h\right)^T z^\theta_h \le \tilde{b} && (4f)
\end{aligned}$$

We denote with $\mathbf{1}^T_N \in \mathbb{R}^N$ the vector of all ones. Eq. (4b) grasps the response of the system operator $y = (g, f, \theta, u)$, with feasible space $\mathscr{Y}$, to an extreme event, a cyberattack, or a compound cyber-physical threat. Notice that the cyberattacker can compromise generation capacity, transmission capacity, and nodal voltage angle limits of the electricity infrastructure network through constraints

(2b)-(2c). Eqs. (4c)-(4e) impose that the cyberattacker strategy (z^g, z^f, z^θ) can not exceed the physical limits of the respective electric power components. Finally, the cyberattacker allocates resources with cost $\tilde{c}_h^g \in \mathbb{R}^{N \times G}$, $\tilde{c}_h^f \in \mathbb{R}^E$, and $\tilde{c}_h^\theta \in \mathbb{R}^N$ to compromise generation capacity, transmission capacity, and nodal voltage angle limits respectively. Notice that increasing vulnerability of an electric power component to a cyberattack decreases the cyberattacker cost. Therefore, parameters $\tilde{c}^g, \tilde{c}^f, \tilde{c}^\theta$ can also be viewed as cyber vulnerability indices. The resources of the cyberattacker are limited to $\tilde{b} \in \mathbb{R}$ in Eq. (4f).

In our formulation, the optimal response of the system operator in Eq. (4b) constrains the cyberattacker optimization problem in Eq. (4). Therefore, the cyberattacker derives the optimal strategy by solving a bilevel optimization problem (Castillo et al., 2019), where the system operator decisions y comprise the lower-level variables and the cyberattacker strategy (z^g, z^f, z^θ) comprise the upper-level variables.

2.3. *Probabilistic Analysis*

In this section, we assume limited publicly available information regarding the cyberattacker capabilities and system-level vulnerabilities of electric power components. For that, in Eq. (5) the cyberattacker cost and budget parameters are uniformly distributed around their mean values $(\bar{b}, \bar{c}^f, \bar{c}^\theta)$, *i.e.,*

$$\tilde{b} \sim \mathscr{U}(\bar{b}), \quad \tilde{c}^f \sim \mathscr{U}(\bar{c}^f), \quad \tilde{c}^\theta \sim \mathscr{U}(\bar{c}^\theta) \qquad (5)$$

Since Eq. (5) is linear, all cost and budget parameter changes are relative to $\bar{c}^g$. We calibrated the mean cyberattacker cost and budget parameters by assuming that under normal operating conditions, the cyberattack goes unnoticed, *i.e.,* compromises no more than 0.5% of NYISO load every hour. Contrary to the NYISO, which oversees transmission infrastructure, electricity generators in the State of New York do not necessarily participate in the cybersecurity initiatives of the North American Electric Corporation (EPRI, 2015). For that, we assumed that generators are more vulnerable than transmission lines. All generators in our model exhibit the same vulnerability to cyberattacks $\bar{c}^g$ across nodes. Similarly, all transmission lines exhibit the same vulnerability to cyberattacks $\bar{c}^f$ and $\bar{c}^\theta$ across edges and nodes.

For the Monte Carlo analysis, we discretized the parameter space of $\bar{b}$ into 15 points, and the parameter space of $\bar{c}^f, \bar{c}^\theta$ into another 15 points. We assumed independence between the parameters and assigned mass probabilities in each point, according to the distributions in Eq. (5). Therefore, our Monte Carlo analysis comprises $15 \times 15 = 225$ experiments.

3. Scenario Design

We modeled the following four scenarios for a 24-hour day during the Fall hurricane season in the NYC Metropolitan area.

Baseline: For the calibration of the OPF, we integrated the four regions of Manhattan (Midtown, Lower-East, Lower-West, North) with the zones of the New York Independent System Operator (NYISO): WEST, GENE, CNTR, NRTH, MHVL, CPTL, HDVL, MLWD, DNWD, NYCN, LNGL. We retrieved the NYISO summer load-duration curve and impedance of all transmission lines from Khan et al. (2022). We retrieved the 2018 NYISO installed capacity from NYISO (2019). Moreover, we considered 19.8 million NYISO customers, according to the earliest known estimate in 2020 (FERC, 2020). We focused on Manhattan as a subregion of the NYISO and assumed that electricity trade with all other system operators is fixed.

Extreme Flooding: Following the extreme flooding scenario in the NYC Stormwater Flood Maps, we assumed 3.5 inches of rain in an hour, which has 1% occurrence probability, and 4.8 feet of sea level rise (NYCOD, 2023). During Hurricane Sandy, four out of six steam generators were inoperable during and immediately after the event (NYC, 2013). For that, we assumed that all power plants in flooded areas are non-functional. Table 1 lists the affected electricity generation facilities in the NYC Metropolitan Area.

Cyberattack: Electricity generation, transmission, and end-use components communicate and operate using Supervisory Control And Data Acquisition (SCADA) devices and Programmable

Table 1: Non-functional power plants under Extreme Flooding.

Generator	Capacity (MW)	Fuel Input
59th Street	37	oil
74th Street	17	gas
East River	716	gas
North 1st	47	gas
Hudson Avenue	109	oil
Gowanus	733	oil
Jamaica Bay Peaking	64	oil

Logic Controllers (PLCs). Therefore, the cyberattacker can compromise generation and transmission capacity by modifying SCADA and PLC firmware (Krishnamurthy et al., 2019; Wang and Karri, 2016) and hardware (Wang et al., 2015, 2016).

Compound Threat: The cyberattacker targets the NYISO during the extreme flooding scenario. Publicly available data on cyberattacks and cyberattackers' capabilities against U.S. electricity infrastructure is extremely limited. For that, we conducted a Monte Carlo analysis by varying the parameters defining the cyberattackers' resources.

4. Results

In this section, we first quantified the compounding impact of a cyberattack during extreme flooding, as compared to a cyberattack under normal operating conditions, for mean cyberattacker capabilities $(\bar{b}, \bar{c}^f, \bar{c}^\theta)$. Then, we conducted a probabilistic analysis to derive the conditional risk profiles of customers and electricity infrastructure components in Manhattan.

4.1. *Cyberattack Compounding Impact*

While the cyberattack under normal operating conditions does not disrupt the electricity supply to NYC, the compound threat exacerbated unserved load by a factor of three. Total unserved load in a 24-hour period grew from 2.59 GWh under the extreme flooding, to 8.15 GWh under the compound threat. Table 2 summarizes our results for a 24-hour period.

The cyberattacker strategy during peak electricity demand at 18:00 provides more insight into the results. During peak demand, the cyberattacker compromised 6.2 GW of fuel capacity in the NYC Metropolitan Area and 17% of transmission capacity between Manhattan and the NYC Metropolitan Area under the compound threat. Extreme flooding incapacitated the East Side gas-fired plant and leads to a 35% unserved load in Midtown Manhattan. The East Side gas-fired plant is the largest electricity generator in Manhattan, thus the extreme flooding rendered Manhattan dependent on electricity imports from the NYC Metropolitan Area. Therefore, curtailing transmission capacity translated into unserved load. Given the compromised generation and transmission capacity, the system operator decides the system configuration that minimizes unserved load in Eq. (4b), which led to shedding 71% of Midtown Manhattan load, affecting approximately 85,181 customers. Figure 2 shows unserved load across Manhattan regions, while Figure 3 shows that the rest of the NYISO zones remained unaffected.

Table 2: Unserved Load (MWh) in Manhattan, 24-hour period. Unserved load under the compound threat is more than three times higher than the sum (column 3) of unserved load under the individual threats.

Extreme Flooding	Cyberattack	Σ	Compound Threat
2.59	0.0	2.59	8.15

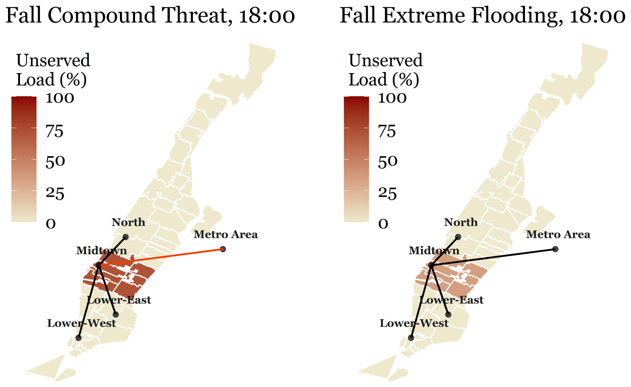

Figure 2: Unserved Load in Manhattan as a percent of Baseline consumption. Targeted transmission lines are in red. The cyberattack exacerbates the unserved load in Midtown Manhattan by a factor of two.

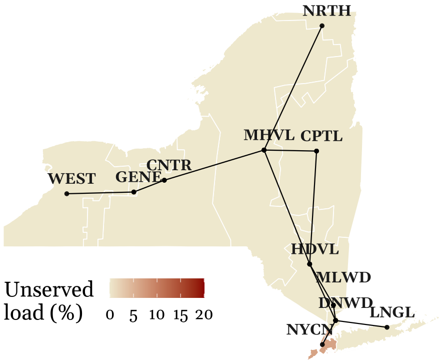

Figure 3: Unserved Load in the NYISO as a percent of Baseline consumption under a compound threat. The NYC Metropolitan Area, including Manhattan, experienced unserved load of 6.6%, while the rest of the NYISO zones remained unaffected.

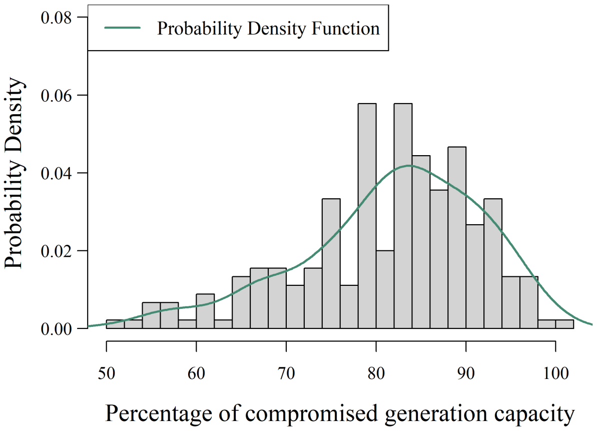

Figure 4: Compromised gas generation capacity under the compound event for the NYC Metropolitan Area. With a probability of 70%, the cyberattacker compromises more than 80% of gas-fired generation in a 24-hour period. We fit a probability density function using the kernel density estimation method.

4.2. *Cyber Risk Profile of Electricity Components*

The probabilistic analysis revealed additional vulnerable regions and infrastructure components under a compound cyberattack and extreme flooding. Figure 4 shows that the cyberattacker targets gas-fired plants in neighboring areas to the flooded regions. The rest of the NYISO generation remains relatively unaffected. In fact, gas-fired plants in the NYC Metropolitan Area were the target of the cyberattacker 80% of the time, as shown in Figure 5.

The cyberattacker targeted components in nodes that are stressed during the extreme flooding, which leads to greater unserved loads in the targeted regions compared to the rest. Lost electricity generation capacity rendered Manhattan dependent on electricity generation from the NYC Metropolitan area. The cyberattacker attempted to curtail electricity supply to Manhattan from neighboring regions by attacking electricity generation in the NYC Metropolitan Area. Gas-fired generators are important to the NYISO network because they have the highest capacity usage factor among all electricity generation technologies in our model. For that, the cyberattacker chose to compromise gas-fired generators first. Moreover, under extreme flooding, electricity generation in Manhattan could no longer support the voltage in the Lower and Midtown Manhattan nodes, which were stressed to their limits. For that, the cyberattacker targeted the voltage angle limit between Manhattan and the NYC Metropolitan Area to constrain flow to Manhattan.

Figure 6 illustrates that beyond Midtown Manhattan, customers in North Manhattan and the NYC Metropolitan Area were also likely to face load shedding. We found that there is a 19% probability that a compound threat during extreme flooding affects more than 129,000 electricity customers in the NYC Metropolitan Area, as shown in Figure 7.

4.3. *Limitations*

The limitations of our analysis arise from the unavailability of publicly available data on critical infrastructure components and cyberattacker capabilities.

First, our analysis is sensitive to the assumptions on transmission line characteristics. Khan et al. (2022) provide a realistic approximation of the NYC and NYISO transmission system. However, additional transmission capacity between Manhattan and the New York City Metropolitan Area can alleviate the impact of a compound threat on the respective interconnections and Manhattan customers.

Second, our analysis is sensitive to the assumptions on the cyberattacker cost parameters, bud-

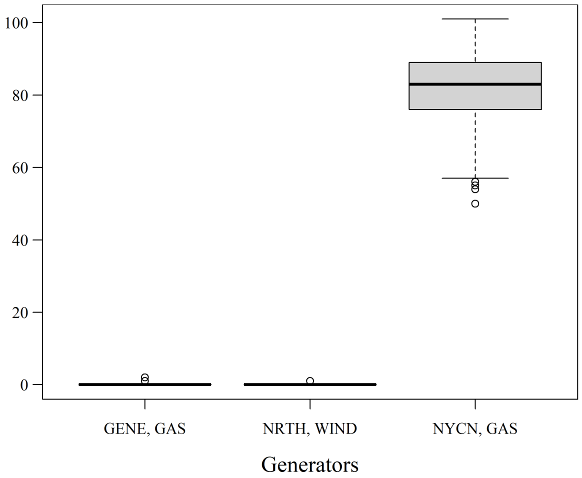

Figure 5: Percentage of compromised generation capacity of the NYISO compared to the Baseline for the top-3 generators.

get, and associated probability distributions. In the absence of information regarding cyberattacker capabilities, the Monte Carlo simulations sample from uniform distributions to explore the parameter space of the cyberattacker optimization problem. Different distributions, also for regionally diverse infrastructure components, can alter the cyber risk profiles under extreme flooding.

5. Conclusion

This work quantifies the risk of cyberattacks against electricity customers and infrastructure components of the NYC Metropolitan area during extreme flooding. We explore the parameter space of the bilevel optimization problem of a cyberattacker through Monte Carlo simulations.

Our analysis is generalizable to multiple regions, natural hazards, and infrastructure systems. The generalization requires identifying the physical vulnerability of regional infrastructure components to earthquakes, hurricanes, and wildfires. Moreover, the formulation in Eq. (2) is a transportation problem. Hence, with minor modifications of Eqs. (2c), (2f), (2h), we can model within the same framework interdependent critical infrastructure systems, including natural gas, biofuel, and food. Future research is necessary to understand the cyberattacker capabilities at the system level.

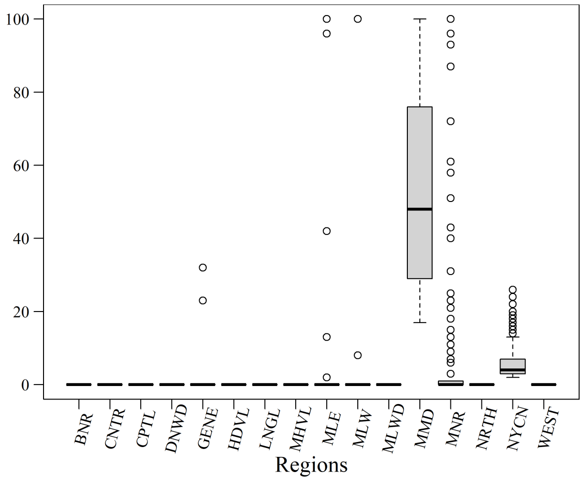

Figure 6: Histogram of the percentage of unserved energy in a 24-hour period in each NYISO zone and Manhattan region compared to the Baseline. Unserved energy in Midtown Manhattan is greater than 80% in 12% of instances. Most NYISO zones remain unaffected.

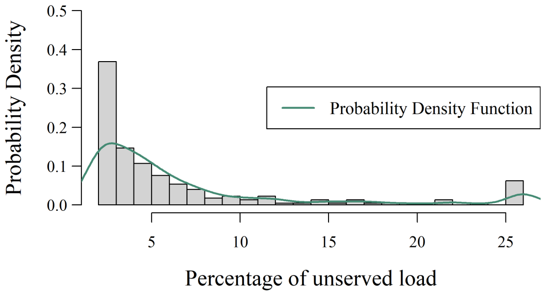

Figure 7: Probability distribution of total unserved energy in the NYC Metropolitan Area in a 24-hour period under varying cyberattacker cost and resources. There was a 19% probability that the unserved energy is higher than 10%, affecting $\sim 129,000$ *customers. We fit a probability density function using the kernel density estimation method.*

6. REFERENCES

Avraam, C., Ceferino, L., and Dvorkin, Y. (2022). "Operational and economy-wide impacts of compound cyberattacks and extreme weather events on electric power networks." *Pre-print*.

Castillo, A., Arguello, B., Cruz, G., and Swiler, L. (2019). "Cyber-physical emulation and optimization of worst-case cyber attacks on the power grid." *2019 Resilience Week (RWS)*, Vol. 1, 14–18.

Eldridge, B., O'Neill, R., and Castillo, A. (2018). "An improved method for the dcopf with losses." *IEEE Transactions on Power Systems*, 33(4), 3779–3788.

EPRI (2015). "Electric Sector Failure Scenarios and Impact Analyses – Version 3.0." *Report No. 3*, Electric Power Research Institute (December). National Electric Sector Cybersecurity Organization Resource (NESCOR).

FERC (2020). "Audit of New York Independent System Operator. Docket No. PA19-1-000.

Khan, H. A. U., Kim, J., and Dvorkin, Y. (2022). "Risk-informed participation in t&d markets." *Electric Power Systems Research*, 202, 107624.

Krishnamurthy, P., Salehghaffari, H., Duraisamy, S., Karri, R., and Khorrami, F. (2019). "Stealthy rootkits in smart grid controllers." *2019 IEEE 37th International Conference on Computer Design (ICCD)*, 20–28.

Mendoza, J. (2023). "Over 135K people are without power from California storm. See where it's hit the most., <https://www.usatoday.com>. Published Jan. 10, 2023. Accessed Feb. 8, 2023.

NCDIT (2018). "Boyette, Thompson Warn of Cyberattacks During Hurricane Florence, <https://it.nc.gov/news/press-releases/>. Published Sept. 14, 2018. Accessed Feb. 8, 2023.

NYC (2013). "A Stronger, More Resilient New York. NYC Special Initiative for Rebuilding & Resiliency.

NYCEM (2019). "NYC's Risk Landscape: A Guide to Hazard Mitigation. NYC Emergency Management.

NYCOD (2023). "New York City Open Data. NYC Stormwater Flood Map - Extreme Flood with 2080 Sea Level Rise. New York City Open Data.

NYISO (2019). "Load & Capacity Data." *Report no.*, New York Independent System Operator, Inc. (April). Gold Book. A report by The New York Independent System Operator, Inc.

Ouyang, M. (2017). "A mathematical framework to optimize resilience of interdependent critical infrastructure systems under spatially localized attacks." *European Journal of Operational Research*, 262(3), 1072–1084.

Sanders, B., Schubert, J., Kahl, D., Mach, K., Brady, D., AghaKouchak, A., Forman, F., Matthew, R., Ulibarri, N., and Davis, S. (2023). "Large and inequitable flood risks in los angeles, california." *Nature Sustainability*, 6, 47–57.

Smith, A. (2021). "2020 U.S. billion-dollar weather and climate disasters in historical context." *Report no.*, National Oceanic and Atmospheric Administration, <https://www.climate.gov/disasters2020>.

Soltan, S., Yannakakis, M., and Zussman, G. (2018). "Power grid state estimation following a joint cyber and physical attack." *IEEE Transactions on Control of Network Systems*, 5(1), 499–512.

Statista (2021). "Annual number of data breaches and exposed records in the united states from 2005 to 2020. Data from Identity Theft Resource Center between 2005 to 2020, excluding non-sensitive records exposed. Accessed: 2022-01-03.

USCB (2021). "U.S. Census 2020.". U.S. Census Bureau.

Wang, X. and Karri, R. (2016). "Reusing hardware performance counters to detect and identify kernel control-flow modifying rootkits." *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 35(3), 485–498.

Wang, X., Konstantinou, C., Maniatakos, M., and Karri, R. (2015). "Confirm: Detecting firmware modifications in embedded systems using hardware performance counters." *2015 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 544–551.

Wang, X., Konstantinou, C., Maniatakos, M., Karri, R., Lee, S., Robison, P., Stergiou, P., and Kim, S. (2016). "Malicious firmware detection with hardware performance counters." *IEEE Transactions on Multi-Scale Computing Systems*, 2(3), 160–173.

Zscheischler, J., Westra, S., van den Hurk, B. J. J. M., Seneviratne, S. I., Ward, P. J., Pitman, A., AghaKouchak, A., Bresch, D. N., Leonard, M., Wahl, T., and Zhang, X. (2018). "Future climate risk from compound events." *Nature Climate Change*, 8, 469–477.