EXPERT WITNESS DECLARATION OF DR. PAUL N. STOCKTON ON BEHALF OF SAN DIEGO GAS & ELECTRIC COMPANY

Dr. Paul N. Stockton

April 9, 2021

I, Dr. Paul N. Stockton, do hereby declare:

1. I am the President of Paul N. Stockton LLC. I make this Declaration on behalf of San Diego Gas & Electric Company (hereinafter referred to as SDG&E) in support of their position in the California Public Utilities Commission (CPUC) Distribution Resources Plan (DRP) proceeding and company policy to treat transmission and substation Geographic Information System (GIS) data, including location with attribution, confidential and not share publicly, even if similar instances of that data have been posted publicly. I have personal knowledge of all matters referred to herein and, if called upon to testify, I could and would competently testify thereto.
2. As President Barack Obama's Assistant Secretary of Defense for Homeland Defense, I was responsible for assessing threats and mitigating threats to defense critical infrastructure. Since leaving office, I have conducted classified and unclassified studies for the Department of Defense's Defense Science Board on the risks that adversaries will attack the power grid and other infrastructure to disrupt the operations of US military bases. I currently serve as the Chair of the Grid Resilience for National Security advisory subcommittee to the Department of Energy and have recently completed a study for the Defense Advanced Research

Projects Agency on cyber threats to transmission systems and power restoration capabilities.

3. I strongly support progress towards clean energy and the accelerated deployment of distributed energy resources (DERs). Continued refinements to California's Integration Capacity Analysis (ICA) algorithms, can help ensure that DER developers have the information they need to design and advance their projects. Those refinements should also account for the increasingly severe threats to the grid from foreign and domestic adversaries, and the risk that adversaries will use transmission system data to help design and conduct their attacks. This declaration provides an analysis of the risks of data exploitation to help ICA policy-makers manage those risks,

and facilitate the *secure* sharing of data between Investor-owned Utilities (IOUs) and DER developers.

4. My declaration begins by examining the threat that China and other foreign adversaries pose to the grid, and especially to the SDG&E transmission systems that serve military bases, electricity-dependent infrastructure essential to public health and safety, and facilities critical to the region's economy. The declaration then assesses the growing risk of attacks on the grid by Domestic Violent Extremists (DVEs). Based on that analysis, the declaration examines how foreign and domestic adversaries could use specific types of data to help plan and execute their attacks, including the exact location of buried and above-ground transmission lines, substations, and related GIS attributes, particularly given the broad reach and impact of this critical infrastructure, to potential high-value targets for adversaries.

5. Attacking the US power grid offers China and other possible foreign adversaries an indirect, and potentially advantageous, means of degrading US defense capabilities. The Department of Defense's *Mission Assurance Strategy* (drafted under my guidance) notes that rather than having to fight highly capable US forces in a conflict zone, adversaries may seek to disrupt the deployment of those forces by crippling the flow of power to US ports, military bases, and other electricity-dependent facilities essential for deployment and support operations.[1]

6. Michele Flournoy, the former Undersecretary of Defense for Policy, warns that China is prepared to conduct just such an attack if a conflict with the US looms over Taiwan. She notes that "Chinese military planning for taking Taiwan by force envisions early cyberattacks against the electric power grids around key military bases in the United States, to prevent the deployment of U.S. forces to the region."[2]

7. These Chinese war plans are of special significance for California and the SDG&E transmission system. Naval Base San Diego is the principal homeport of the Pacific Fleet, consisting of 46 Navy ships, Coast Guard cutters, seven Military Sealift Command logistical support platforms, and several research and auxiliary vessels. Naval Base San Diego is home to 213 individual commands, each having specific and specialized fleet support purposes.[3] These commands would be essential for deploying and sustaining the Pacific Fleet in future conflicts. All of them rely on

[1] Department of Defense, *Mission Assurance Strategy*, April 2012, https://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf

[2] Michele Flournoy, "How to Prevent a War in Asia: The Erosion of American Deterrence Raises the Risk of Chinese Miscalculation," *Foreign Affairs*, June 18, 2020, p. 5, https://www.foreignaffairs.com/articles/united-states/2020-06-18/how-prevent-war-asia

[3] US Navy, Naval Base San Diego, https://www.cnic.navy.mil/regions/cnrsw/installations/navbase_san_diego.html

power provided by the SDG&E transmission system, and on the distribution substations and other infrastructure that provide the "last mile" of service to these commands.

8. SDG&E transmission and distribution systems also power a wide range of other military installations, including Marine Corps Base Camp Pendleton and the Naval Warfare Information Command Pacific, which identifies, develops, delivers and sustains information warfighting capabilities and services that enable naval, joint, coalition and other national missions operating in warfighting domains from seabed to space.[4] In addition, electric power from SDG&E systems is vital to sustain the combat support functions and other services provided by defense contractors in the region, including BAE Systems, Huntington Ingalls Industries Inc, and General Dynamics.

9. Former Undersecretary Flournoy emphasizes that Chinese attacks on the grid could not only disrupt the deployment of US forces to the conflict zone, but also hospitals, emergency services, and other functions critical to public safety. The US Intelligence Community (IC) has determined that disrupting the flow of power to facilities essential for public health and safety fits into the broader strategies of Russia, China, and other potential adversaries. According to the *National Counterintelligence Strategy of the United States, 2020-2022*, which provides the most detailed US Intelligence Community (IC) assessment of adversary goals in such cyber-related activities, "adversaries are conducting intelligence operations to exploit, disrupt, and damage U.S. and allied critical infrastructure and military

[4] Naval Information Warfare Systems Command Pacific, https://www.navwar.navy.mil/about/

capabilities during a crisis." Those efforts "likely are aimed at influencing or coercing U.S. decision makers in a time of crisis by holding critical infrastructure at risk of disruption."[5] Other Federal threat assessments warn that adversaries may seek to cripple defense-related assets as well as hold the public survival at risk. The Office of the Director of National Intelligence has warned that Russia is "staging cyber attack assets to allow it to disrupt or damage US civilian and military infrastructure during a crisis" along with posing "a significant cyber influence threat" to shape US behavior.[6]

10. Holding the electric grid at risk would offer an especially potent source of leverage. The *Counterintelligence Strategy* warns that because of the importance of the US electric systems to the economy and public health and safety, those systems could offer a prime target. Indeed, "adversaries seeking to cause societal disruption in the United States could attack the electrical grid causing a large-scale power outage that affects many aspects of daily life."[7] Given the role of transmission systems in providing electricity for delivery by distribution-level infrastructure to hospitals, water systems, and other critical customers, those systems will be key targets for adversaries seeking to create such large-scale outages.

11. The SDG&E services area includes numerous electricity-dependent facilities essential to public health and safety. The Scripps Mercy Hospital in San Diego provides Level-1 trauma care to the region. The San Diego County Water Authority

[5] National Counterintelligence and Security Center (NCSC), *National Counterintelligence Strategy of the United States of America 2020-2022*, Washington, DC: NCSC, February 2020, pp. 8 and 6, https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf.NCSC, *National Counterintelligence Strategy*.
[6] Daniel R. Coats, *Worldwide Threat Assessment of the US Intelligence Community*, Washington, DC: ODNI, January 29, 2019, 5, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.
[77] Counterintelligence Strategy, p. 6.

and other regional agencies operate multiple pumping stations, a desalination plant, water treatment facilities, wastewater plants, and other infrastructure that depends on electricity to function. Some of these facilities have emergency generators and on-site fuel storage that can enable them to function in relatively brief outages. However, if China or other adversaries can target their attacks to create longer-term disruptions of service to these facilities, their ability to save and sustain lives would be in growing jeopardy.[8]

12. The Counterintelligence Strategy emphasizes that opponents may also focus their attacks on infrastructure systems essential to the US economy.[9] Transmission lines and substations offer potentially valuable targets in this regard. If adversaries can halt the flow of power to defense companies in the San Diego region, for example, they can not only degrade the ability of those companies to provide key military support services but also disrupt the $25 billion in economic activity and many thousands of jobs that these companies contribute to the local economy.[10] On a cumulative basis, the Defense Department estimates that in 2019 the military was responsible for over $28 billion in direct spending to the San Diego region, which resulted in a Gross Regional Product of over $51 billion, or 22%, of San Diego's Gross Regional Product (GRP) -- more than tourism or privately funded research

[8] Federal Emergency Management Agency, Power Outage Incident Annex to the Response and Recovery Federal Interagency Operational Plans: Managing the Cascading Impacts from a Long-Term Power Outage, June 2017, https://www.fema.gov/sites/default/files/2020-07/fema_incident-annex_power-outage.pdf
[9] Counterintelligence Strategy, p. 6.

[10] Propel San Diego, *Mapping San Diego's Defense Ecosystem*, February 2018, https://www.sandiegobusiness.org/sites/default/files/Mapping%20San%20Diego%27s%20Defense%20Ecosystem.pdf

and development.[11] Disrupting the transmission infrastructure that make these contributions to the economy possible offers can adversaries a potentially immense source of coercive leverage in future confrontations. The same is true of halting electric service to San Diego International Airport (worth $12 billion annually to the region's economy) and other civilian facilities and functions served by SDG&E.[12]

13. This declaration has focused thus far on threats to California's transmission systems from China and other potential foreign adversaries. However, the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS) and other agencies warn that US infrastructure also face intensifying threats from Domestic Violent Extremists (DVEs) and other US-based attackers. Accounting for these domestic threats is essential to assessing the risks posed by the public display of data on the exact location of substations, power lines, and other transmission infrastructure and information.

14. According to a March 2021 Report by the Office of the Director of National Intelligence, "the IC assesses that racially or ethnically motivated violent extremists (RMVEs), and militia violent extremists (MVEs) present the most lethal DVE threats," with MVEs typically targeting law enforcement and government

[11] US Department of Defense, Office of Economic Adjustment, Project Profile: San Diego, 2019, https://crecstorage.blob.core.windows.net/crec/2020/07/San-Diego-CA-Profile-2019-Final.pdf

[12] Ken Stone, "Annual Economic Value of San Diego's Airport? Nearly $12 Billion, Study Says," *Times of San Diego*, September 18, 2018, https://timesofsandiego.com/business/2018/09/18/annual-economic-value-of-san-diegos-airport-nearly-12-billion-study-says/

facilities and personnel.[13] Extremists seeking to disrupt these facilities and cause vivid, widespread societal disruptions can also attack the electric infrastructure on which the facilities depend. Moreover, while sophisticated cyberattacks require capabilities that are beyond the reach of most terrorist organizations, kinetic weapons and material for improvised explosive devices (IEDs) are readily available to domestic actors.

15. Grid resilience stakeholders in California are well aware of the risk that even high-powered rifle attacks can pose to transformers and substations. The 2013 attack on the Metcalf, California substation highlighted those risks. In a comprehensive 2015 study of physical security and regulatory options conducted by the staff of the California Public Utilities Commission (CPUC), the authors found that while no customers lost power due the event, "a similar attack under different circumstances might have been catastrophic."[14] The CPUC staff report documented other physical attacks on grid infrastructure as well in California and beyond.

16. Since publication of the staff's report, such attacks have become more frequent and increasingly ambitious. In the 2016 rifle attack against the Buckskin substation in central Utah and other operations, the use of small arms fire against transformers has become especially concerning.[15] Replacing transformers is a lengthy process.

[13] Office of the Director of National Intelligence, Domestic Violent Extremism Poses Heightened Threat in 2021, March 1, 2021, https://www.dni.gov/files/ODNI/documents/assessments/UnclassSummaryofDVEAssessment-17MAR21.pdf

[14] Ben Brinkman, et al, *Regulation of Physical Security for the Electric Distribution System February*, California Public Utilities Commission Staff Report, February 2015, iii.

[15] Peter Behr, "Substation attack is new evidence of grid vulnerability, *E&E News*, October 6, 2016, https://www.eenews.net/stories/1060043920

Successful, coordinated attacks on them at scale could create long duration outages. The Department of Energy notes that transformers are "one of the most vulnerable components on the grid." While utilities do maintain some in reserve, transformers "are generally expensive, difficult to transport, and typically custom-made with procurement lead times of one year or longer."[16]

17. Terrorist groups can scale up the resulting threats to grid infrastructure by seeking to strike multiple substations in a single operation. The "Lights Out" campaign exemplifies these risks. According to a December 2020 FBI affidavit that was mistakenly unsealed, white supremacists have been plotting to attack multiple substations with rifle fire in Colorado and the southeastern United States.[17] If extremist groups coordinated equivalent attacks against Californian substations, and utilities needed to replace multiple transformers within them, the state could face long duration, wide area power outages.[18]

18. The FBI affidavit also stated that the plotters sought to gather data from DOE websites to help plan their attack.[19] Fortunately, DOE has stringent rules to protect Critical Electric Infrastructure Information (CEII) from unauthorized access. Equivalent data security measures, tailored to meet the needs of California while also facilitating energy development projects, will be essential to impede attack planning by extremist

[16] DOE, Addressing Security and Reliability Concerns of Large Power Transformers, https://www.energy.gov/oe/addressing-security-and-reliability-concerns-large-power-transformers. While the report focuses on large power transformers, as opposed to smaller transformers used in many distribution substations, many of the vulnerabilities and replacement challenges cited in the report apply to both categories.
[17] Amy Forliti, White supremacists plotted to attack US electric grid by shooting into power stations, FBI says, US News, December 22, 2020, https://www.usatoday.com/story/news/nation/2020/12/22/white-supremacists-plotted-attack-us-power-grid-fbi-says/4018815001/
[18] Rick Sallinger "'Lights Out': Neo-Nazi Plot To Disable Power Grid Allegedly Included Attacking Substation In Colorado," *CBS Denver*, December 23, 2020, https://denver.cbslocal.com/2020/12/23/lights-out-neo-nazi-plot-disable-power-grid-allegedly-included-attacking-substation-colorado/
[19] *Ibid.*

groups. This analysis that follows in this declaration examines the specific types of data that could be most valuable to domestic and foreign adversaries for attack planning and execution.

19. The 2015 CPUC staff report on physical security found that protecting sensitive information could play a major role in securing the grid, and that "it is important that all documents receive careful screening before any public release."[20] Subsequent CPUC actions, including those associated with Physical Security of Electric Infrastructure (R.15-06-009), have continued to help strengthen grid resilience.[21] However, as noted in the CPUC Staff White Paper on *Security and Resilience of California Electric Distribution Infrastructure: Regulatory and Industry Responses to SB 699* (January 2018), the question of how to strike a balance between the goals of making data available to the public and ensuring grid security remains at issue. As the report states, "The crux of the issue here appears to be (H)ow to balance disparate and well-intended, but seemingly conflicting goals surrounding the Commission's responsibility to protect the public and the Commission's responsibility to provide the public with access to information?[22]

20. Taking a risk-based approach, the data that would be most helpful to adversaries in planning and conducting high-consequence attacks should merit the most

[20] CPUC Staff report, 38. See also p. 16 above Malashenko, Elizaveta, Chris Villarreal, and J. David Erickson. Cybersecurity and the Evolving Role of State Regulation: How It Impacts the California Public Utilities Commission. San Francisco, CA: California Public Utilities Commission, August. 2014, p. 16 and passim, https://www.cpuc.ca.gov/uploadedFiles/CPUC_Website/Content/Utilities_and_Industries/Energy/Reports_and White_Papers/TheEvolvingRoleofStateRegulationinCybersecurity9252012FINAL.pdf

[21] California Public Utilities Commission, Physical Security of Electric Infrastructure (R.15-06-009), https://www.cpuc.ca.gov/General.aspx?id=6442453847

[22] Jeremy Battis et al, CPUC Staff White Paper on *Security and Resilience of California Electric Distribution Infrastructure: Regulatory and Industry Responses to SB 699*, January 2018, p. 46, https://www.cpuc.ca.gov/uploadedFiles/CPUCWebsite/Content/Safety/Risk_Assessment/physicalsecurity/Final%20CPUC_Physical_Security_White_Paper_January_2018(1).pdf

stringent measures for secure sharing with DER developers. Strategic data on the exact physical location of transmission assets along with attributes and interconnections, beyond high-level locational satellite imagery, provides a case in point.

21. For DVEs and other adversaries seeking to create wide area, long duration outages locational information on substations and transmission lines (both above ground and below) can be especially useful. As noted above, the Lights Out plotters sought detailed information on the layout transmission systems to design their attack. A detailed display of system topology – that is, the structure and layout of an electric system – is a potential goldmine for adversaries seeking to focus physical attacks on specific assets for maximum disruption.[23] A growing number of studies also examine how attackers can use data gathered on typology of grid networks, transmission lines and other physical assets, and load data to design and execute potentially catastrophic attacks.[24]

---

[23] For definitions of grid topology and the data it encompasses, see DOE, National Transmission Grid Study, May 2002, https://www.ferc.gov/sites/default/files/2020-04/transmission-grid_0.pdf

[24] Y. Sun, W. Li, W. Song and C. Yuen, "Joint cyber and physical attacks against topology of electric grids," *2016 IEEE Region 10 Conference (TENCON)*, Singapore, 2016, pp. 746-750, 10.1109/TENCON.2016.7848103; Jiazi Zhang, "Topology Attacks on Power System Operation and Consequences Analysis," June 2015, https://repository.asu.edu/attachments/158045/content/Zhang_asu_0010N_15269.pdf; D. Deka, R. Baldick and S. Vishwanath, "One breaker is enough: Hidden topology attacks on power grids," *2015 IEEE Power & Energy Society General Meeting*, Denver, CO, USA, 2015, pp. 1-5, 10.1109/PESGM.2015.7286568; Song, Y., Liu, X., Li, Z. *et al.* "Intelligent data attacks against power systems using incomplete network information: a review." *J. Mod. Power Syst. Clean Energy* **6,** 630–641 (2018). https://doi.org/10.1007/s40565-018-0427-z

22. Sophisticated new analytic tools are also increasing the value of publicly available data for grid attack planning. The US National Science and Technology Council has found that AI, machine learning, and other advances can help cyber defenders enhance their protection operations. But the council also notes that AI will help attackers make more effective use of the data they gather, by helping model a victim's systems, and develop plans to exploit the vulnerabilities that AI helps identify.[25] China has declared its intention to become the world leader in AI, and is committed to applying its expertise to "leapfrog" U.S. defense capabilities.[26] Russia is also ramping up its AI research and development efforts. The net effect of these analytic advances: publicly available information that once might have provided only a limited basis for cyber and physical attack planning is now increasingly valuable.

23. Efforts to assess the risk posed by adversary exploitation of sensitive data should also account for the risk that adversaries will use highly destructive means to counter the measures taken by IOUs to comply with the cyber and physical Critical Infrastructure Protection (CIP) standards maintained by the North American Electric Reliability Corporation (NERC) .[27] Very large scale truck bombs and other improvised explosive devices (IEDs) provide a case in point. In 2014, attackers

---

[25] AI and Cybersecurity: Opportunities and Challenges, National Science and Technology Council, March 2020, p. 5, https://www.nitrd.gov/pubs/AI-CS-Tech-Summary-2020.pdf. See also Greg Allen and Daniel Chan, Artificial Intelligence and National Security, Belfer Center for Science and International Affairs, July 2017, p. 24, https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf.

[26] Elsa B. Kania , Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power, Center for a New American Security, November 2017, p. 4, https://s3.amazonaws.com/files.cnas.org/documents/Battlefield-Singularity-November2017.pdf?mtime=20171129235804.

[27] NERC has also established CIP standards to protect sensitive data. In particular, CIP-011-1, *Information Protection*, is structured "To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES." North American Electric Reliability Corporation, CIP -011-1, *Information Protection*, https://www.nerc.com/files/CIP-011-1.pdf. Note that NERC has issued subsequent modifications to CIP-011-1 to further clarify and expand upon the initial standard.

placed a makeshift bomb next to a 50,000-gallon diesel tank at a substation near Nogales, Arizona. The bomb caused only minor damage because it failed to ignite the diesel fuel (which has a high flash point and is difficult to ignite). However, law enforcement officials stated that had there been a catastrophic explosion, as many as 30,000 customers could have lost power for an extended period.[28]

24. The December 2020 explosion in Nashville, TN offers a more recent example of the destructiveness of IEDs and the regional effects lone actors can create. A recreational vehicle exploded in front of an AT&T Inc. switching station, knocking out a central node that directs data from users and businesses across telecom systems.[29] AT&T customers lost service across wide areas of Tennessee, Kentucky, and Alabama, and halted 911 call services and other critical functions. The company quickly established portable cell sites to accelerate restoration of service.[30] However, if adversaries can target equivalent attacks against one or more critical electric infrastructure assets (CEI) in California, they may be able to create extensive, long duration outages.

25. These risks extend to the public release of data on buried transmission lines. Buried lines are typically more resilient against natural hazards and, potentially, physical

[28] Sean Holstege and Ryan Randazzo, "Sabotage at Nogales station puts focus on threats to grid," *AZ Central*, June 12, 2014, https://www.azcentral.com/story/news/arizona/2014/06/12/sabotage-nogales-station-puts-focus-threats-grid/10408053/The law enforcement sources for the article did not specify the length of the outage that an explosion could have created. A number of factors determine outage durations, including the avaiablity of alternative substations and power feeds to serve the stricken area, and possible use of mobile emergency assets to accelerate service restoration. In typical radial distribution systems, however, the catastrophic destruction of a critical substation could produce extended blackouts.

[29] David Umberti, "Nashville Bombing Exposes Weak Point for Business Communications," *Wall Street Journal*, December 28, 2020, https://www.wsj.com/articles/nashville-bombing-exposes-weak-point-for-business-communications-11609194817

[30] Tali Arbel, Nashville Bombings Spotlight Vulnerable Voice, Data Networks," Associated Press, December 29, 2020, https://apnews.com/article/service-outages-bombings-nashville-a14babd6748fea7c43ed396801aaabf7

attacks that overhead lines. But large scale truck bombs can disrupt all but the most deeply buried and extensively hardened lines. For example, in the 1995 attack on the Oklahoma City Federal Building, the truck bomb blasted a crater eight feet deep and 20 feet in diameter.[31]

26. Extremist groups could further disrupt power restoration and achieve wider area outages by coordinating IED attacks against multiple transmission substations. In September 2017, a leader of the extremist organization Atomwaffen Division (AWD), issued a call to attack substations and bragged that he had a West Coast grid map provided by "someone with special permissions to get it." After another AWD member claimed that the group was planning to use a cache of explosives to attack the grid and other targets, the FBI arrested five members across four different states in April, 2020.[32]

27. DHS warns that lone actors and terrorist organizations may also use more advanced weapons in future attacks. While the use of rudimentary explosive devices will probably remain most common, "lone offenders could employ more sophisticated means, to include advanced and/or high-consequence IEDs" and other types of attacks." In particular, "terrorists and other criminal actors might look to unmanned aircraft systems (UAS) to threaten critical infrastructure."[33] Protecting locational

[31] Sue Anne Pressley, "Bomb Kills Dozens in Oklahoma Federal Building, *Washington Post*, April 20, 1995, https://www.washingtonpost.com/wp-srv/national/longterm/oklahoma/stories/firststory.htm#:~:text=Debris%20from%20the%20blast%20formed,that%20was%20filled%20with%20rubble.

[32] K. Campbell, "The Far-Right Domestic Extremist Threat to the Power Grid," *Homeland Security Today*, March 24, 2020, https://www.hstoday.us/subject-matter-areas/infrastructure-security/the-far-right-domestic-extremist-threat-to-the-power-grid/

[33] *Homeland Threat Assessment*, Department of Homeland Security, October 2020, 9917-19 https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf

information that attackers might use to target substations and other assets with these advanced weapons can make a significant contribution to the security of California's transmission infrastructure.

28. Exploitation of public available data poses challenges to transmission cybersecurity as well. As noted above, system topology and information on data power flows can aid adversaries in designing their attacks, especially with the use of new AI tools to assist such planning. US researchers have identified a number of ways in which data gathered on the web can be used to profile the network structure and other structural characteristic of US power companies.[34] DRAGOS, a leading cybersecurity firm, has leveraged the Department of Defense's CARVER data matrix to identify categories of open source information that attackers can find especially valuable for attack planning. One such category is "critical information" that "informs an adversary of the impact of an attack for the target's continued operation. A target's criticality is determined if its compromise or destruction has a highly significant impact in the overall organization and its ability to conduct business or operations." A closely related category is that of "effect information," that is, information about the amount of direct or indirect loss a target would have from an attack or compromise," and its ability to operate.[35] Under this framework, open source information of special concern would include data that could help adversaries target attacks against substation, power lines, and other transmission

[34] Darren Hayes, Using Open Source Intelligence for Risk Assessment to the U.S. Power Grid, April 2017, https://www.researchgate.net/publication/316167221_USING_OPEN_SOURCE_INTELLIGENCE_FOR_RISK_ASSESSMENT_TO_THE_US_POWER_GRID.

[35] Selena Larson, Open Source Intelligence, DRAGOS, Inc, December 2020, https://www.dragos.com/resource/open-source-intelligence/.