China’s Government Is Learning From Russia’s Cyberattacks Against Ukraine

recordedfuture.com/chinas-government-is-learning-from-russias-cyberattacks-against-ukraine/

Insikt Group

Chinese government entities, state-owned enterprises, and cybersecurity researchers have demonstrated a practical interest in the 2015 cyberattack against Ukraine’s power grid as well as subsequent attacks, which have been credibly attributed to Sandworm Team, a Russian state-sponsored advanced persistent threat group. Recorded Future has found that procurement documents associated with various Chinese government entities and state-owned enterprises have referenced the attack, with several documents explicitly calling for cybersecurity capabilities to counter or simulate such an attack. Likewise, cybersecurity researchers associated with the People’s Liberation Army (PLA), state-run research organizations, and other such entities have discussed the implications of the incident in their ongoing technical research, highlighting the national security relevance of protecting critical infrastructure and the prominence of this infrastructure as a target in interstate conflict. Together, these sources suggest that relevant parties in China recognize the conceptual significance of the 2015 attack on Ukraine’s grid and are very likely factoring lessons from the incident (such as the acute need to defend critical infrastructure against state-sponsored cyber threats) into their cybersecurity planning. The evidence presented in this report suggests that the Chinese authorities are almost certainly watching and learning from Russia’s ongoing war in Ukraine and any accompanying cyber activity.

Cyberattacks on Ukraine’s Power Grid

On December 23, 2015, a cyberattack against Ukraine’s grid targeted 3 regional electric power distribution companies and disrupted the supply of power to 225,000 customers. Reporting on the incident described it as the “first known successful cyber intrusion to knock a power grid offline”. Another cyberattack hit Ukraine’s grid in 2016, knocking out a portion of Kyiv’s power. In October 2020, the US Department of Justice (DOJ) charged several officers in Unit 74455 of Russia’s Main Intelligence Directorate (GRU) in connection with the attacks on Ukraine’s power grid and other Sandworm Team activity. According to the US DOJ, these

GRU officers carried out “destructive malware attacks against Ukraine’s electric power grid, Ministry of Finance, and State Treasury Service, using malware known as BlackEnergy, Industroyer, and KillDisk” from December 2015 through December 2016.

Chinese Government and State-Owned Enterprise Interest in the 2015 Attack

Procurement documents from the past several years reveal that government entities and state-owned enterprises in China have almost certainly incorporated lessons from the 2015 Ukraine attack (and possibly later incidents) into their cybersecurity planning. These organizations have demonstrated both abstract interest in the attack, naming it as an example of the current cyber threat landscape, and specific interest in seeking the capability to simulate or otherwise counter the tactics, techniques, and procedures used to target Ukraine’s grid. Instances that Recorded Future identified include:

- In March 2022, the Guangxi Zhuang Autonomous Region (GZAR) Natural Resources Remote Sensing Institute (广西壮族自治区自然资源遥感院) published a tender for an “AI [artificial intelligence] high-performance data solution server”. The GZAR Natural Resources Remote Sensing Institute is subordinate to the GZAR Department of Natural Resources. A technical requirements list attached to this tender states that the server should have third-party (unspecified) antivirus software with the capability to trace advanced threats such as the “Ukraine power cut incident”.
- In September 2020, Guangdong Province Wind Power Generation Co., Ltd. (广东省风力发电有限公司) released a tender for a “wind farm power monitoring and control system grade protection 2.0 compliance reform” project. Guangdong Province Wind Power Generation is a state-owned enterprise. The document references the 2015 attack on Ukraine’s grid as an example of a major information security threat to critical infrastructure.
- In November 2019, the Suzhou City Public Security Bureau (苏州市公安局) released a tender for “antivirus gateway and antivirus handling services”. The document discusses the growing importance of digital infrastructure and the protection of this infrastructure, referencing cyberattacks such as one of the attacks on Ukraine’s power grid. The document also mentions that China’s Golden Shield Project — an extensive online surveillance capability run by the Ministry of Public Security (MPS) — has a “national virus early warning and reporting management mechanism”.
- In September 2019, China Southern Power Grid Co., Ltd. (中国南方电网有限责任公司) released a tender for “power monitoring and control system network security intelligent analysis application V1.0 construction project technical services”. China Southern Power Grid is a state-owned enterprise. The document references the 2015 attack against Ukraine’s grid as an example of the growing threat against grid control systems.

- In March 2019, the Shenzhen City Information Security Testing and Evaluation Center (深圳市信息安全测评中心) published requirements for an “industrial internet attack and defense exercise platform”. The document identifies the capability to “simulate the 2015 Ukraine power grid security incident” as one of the requirements for the project’s “industrial control power attack tool kit”.

In addition to paying attention to the 2015 attack, certain Chinese state-owned enterprises likely have a more direct interest in grid security in Ukraine. For instance, Ukraine’s Donbasenergo reportedly contracted Dongfang Electric Corporation (中国东方电气集团有限公司) in 2018 for work on the Sloviansk thermal power plant, with the upgraded units initially projected to start producing power in 2022 or 2023. Similarly, China Longyuan Power Group (龙源电力集团股份有限公司) reportedly “has a 76.6-megawatt wind power project in Yuzhne on the country's Black Sea coast in the Southwest, which started operation last year as the company's first wind power project in Europe”, according to state media. Likewise, a January 2020 procurement document shows that China National Nuclear Corporation (CNNC) Environmental Protection Industry Co., Ltd. (中核环保产业有限公司) was seeking to station engineers on a long-term basis in locations like Kramatorsk, Ukraine, and Saint Petersburg, Russia.

References to the 2015 Attack in Chinese Cybersecurity Research

Various cybersecurity researchers affiliated with the PLA, state-run research organizations, and other such entities in China have also recently discussed the implications of the 2015 attack on Ukraine’s power grid — as well as the implications of subsequent cyberattacks against Ukraine’s critical infrastructure. This research does not necessarily reflect official PLA, Chinese government, or Chinese Communist Party (CCP) institutional positions but does offer a degree of insight into how specialists positioned within these institutions have reacted to (and are continuing grapple with) the 2015 Ukraine attack and other associated incidents. In particular, researchers stress the national security implications of the 2015 attack and highlight how cyberattacks against critical infrastructure are now a feature of interstate conflict. Recent examples include the following:

- In the February 2022 issue of the *Journal of Beijing University of Aeronautics and Astronautics* (北京航空航天大学学报), researchers associated with the State Grid Henan Electric Power Research Institute (国网河南省电力公司电力科学研究院) and PLA Strategic Support Force (PLASSF) Information Engineering University (中国人民解放军战略支援部队信息工程大学) describe the 2015 Ukraine attack as the first instance of a “hacker penetration” leading to a large-scale power outage incident and argue that “how to ensure the security and stable operations of power grid control systems has already become a major research issue for each country’s protection of national security”. The authors use this assessment to frame their research on smart grid network threat evaluation.

- In the January 2022 issue of *Network Security Technology & Application* (网络安全技术与应用), researchers from Purple Mountain Laboratories (网络通信与安全紫金山实验室) and PLASSF Information Engineering University mention the 2015 Ukraine grid attack alongside other incidents as proof of the growing threat against industrial control systems across the globe. The authors use this assessment to frame their research on industrial control system honeypots.
- In the November 2021 issue of the *Journal of Computer Research and Development* (计算机研究与发展), authors affiliated with the Harbin Institute Technology Cybersecurity Research Institute (哈尔滨工业大学网络空间安全研究院), China Information Technology Security Evaluation Center (CNITSEC; 中国信息安全测评中心), and other organizations referenced the 2015 cyberattack on Ukraine’s power grid as clear evidence of industrial control networks having become a major target in interstate conflict. The authors use this assessment to frame their research on industrial control network multi-mode attack detection and evaluation.
- In the February 2019 issue of *Systems Engineering and Electronics* (系统工程与电子技术), researchers associated with the Air Force Engineering University School of Information and Navigation (空军工程大学信息与导航学院) and PLA Unit 93801 (中国人民解放军93801部队) describe cyberattacks against Ukraine’s computer networks and power grid as examples of incidents driving increasing research interest in the stability and security of “multiple elements state cyberspace”. The authors use this assessment to frame their research on the simulation of risk propagation in “multiple elements military state cyberspace”.

Outlook

The evidence presented in this report suggests that government entities, state-owned enterprises, and cybersecurity researchers in China recognize the significance of Russia’s attacks on Ukraine’s power grid and are working to defend China’s critical infrastructure against similar attacks, including in the context of interstate tensions or conflict. While all of the sources reviewed in this report discuss defensive measures, Chinese strategists very likely view offensive and defensive cyber activity as two sides of the same coin. Moreover, Recorded Future previously observed China-linked threat activity group RedEcho targeting India’s power sector during the 2020 India-China border tensions, a real-world demonstration of China’s willingness to target other countries’ critical infrastructure. As such, not only are relevant parties in China using lessons from Russia’s cyber activity in Ukraine to inform cybersecurity planning, but these entities might also be drawing insights related to offensive cyber planning.