Advanced Persistent Threats on Consumer Energy Resources in Decentralized Energy Systems

Kaibin Bao
KIT
Karlsruhe, Germany
kaibin.bao@kit.edu

Sid Chi-Kin Chau
CSIRO Data61
Sydney, Australia
sid.chau@acm.org

Ghada Elbez
KIT
Karlsruhe, Germany
ghada.elbez@kit.edu

Qi Liu
KIT
Karlsruhe, Germany
qi.liu@kit.edu

Veit Hagenmeyer
KIT
Karlsruhe, Germany
veit.hagenmeyer@kit.edu

Abstract

With the increased share of renewable energy sources in energy infrastructures worldwide, power grids are shifting toward decentralization, in which Consumer Energy Resources play an important role. However, due to their reliance on digitization and Internet connectivity, Consumer Energy Resources significantly broaden the attack surface on power grids. Coordinated cyberattacks from in particular Advanced Persistent Threats may cause not only economical but also societal impacts. In this paper, we first describe the capabilities of these attackers. Then we illustrate the most likely attack paths and analyze the potential impacts. Subsequently, we present some potentially promising countermeasures. We conclude this paper by raising several open questions for future work.

Keywords

Cyberattacks, Advanced Persistent Threats, Decentralized Energy Systems

ACM Reference Format:
Kaibin Bao, Sid Chi-Kin Chau, Ghada Elbez, Qi Liu, and Veit Hagenmeyer. 2025. Advanced Persistent Threats on Consumer Energy Resources in Decentralized Energy Systems. In *The 16th ACM International Conference on Future and Sustainable Energy Systems (E-ENERGY '25), June 17–20, 2025, Rotterdam, Netherlands.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3679240.3734653

1 Introduction

Driven by net-zero emissions targets, the share of energy produced from renewable sources worldwide has risen from 18% to 30% in the past 20 years [16]. The share of solar energy grew from 0.02% to 5.53% globally, with nations like Germany and Namibia seeing solar energy's share rise from nearly 0% to 12% and 37%, respectively [17]. In several Australian states, solar energy supplies as much as 75% of total electricity at times [4].

This trend is fueled by the fast-growing market for residential and commercial rooftop solar panels [48], making home and business owners significant contributors to power generation and management. A photovoltaic system is the most prominent Consumer Energy Resource (CER), a category of small-scale, consumer-owned or -controlled energy assets, such as rooftop solar panels, home batteries, and smart appliances. These assets can generate, store, or manage electricity to actively participate in the grid by providing flexible load or generation. However, unlike conventional power plants, distributed CERs rely on digitization and Internet connectivity, which enlarges the power grids' cyberattack surface. A coordinated cyberattack across many decentralized systems could jeopardize grid stability and even result in blackouts.

Advanced Persistent Threats (APTs) — often state-sponsored and equipped with zero-day exploits, specifically crafted malware, and sophisticated hacking tools — pose an escalating threat to critical infrastructures. Such attackers can evade defense systems, gain persistent access, and move laterally within compromised systems. Documented incidents reveal infiltrations of telecommunication networks, government institutions, industrial control systems as well as other critical infrastructures worldwide [44, 56], with Stuxnet standing out as a prominent example [26, 30].

Threat actors have demonstrated their ability to control large botnets, using them for extensive distributed denial-of-service attacks or as a launchpad for deeper intrusions [52, 53]. The widespread deployment of poorly secured Internet of Things (IoT) devices [5] inevitably opens local area networks including CER devices in residential and commercial buildings to malicious access. After obtaining an initial foothold in target networks, advanced attackers with enough resources and expertise can maximize the compromise of these networks and the associated devices, eventually gaining the ability to orchestrate large-scale disruptions to the power grids.

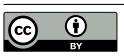
In this paper, we aim to first raise the awareness of potential APT attacks on decentralized energy systems in the near future by introducing a few past APT attacks on energy systems and analyzing the capabilities of APT actors. Then we describe some most likely attack paths of these threat actors inside decentralized energy systems, in which we take residential rooftop photovoltaic systems as a concrete example for CERs. In such a system, the inverter is the major CER device connected to the power grid both electrically and digitally, and its power electronics allow the most versatile impact on the electrical grid. We also analyze the potential impacts of these attacks on energy systems. Subsequently, we make suggestions on how these attacks could be fended off, or prevented. Finally, we raise some open questions for future work to address.

2 Past Incidents & APT Capabilities

In the last decade, several cases of cyberattacks conducted by APT actors have been observed and studied, highlighting their sophisticated and evolving nature.

2.1 Cyberattacks Targeting Energy Systems

In the following, we survey a few past incidents of APT attacks targeting energy systems:



E-ENERGY '25, Rotterdam, Netherlands

ACM ISBN 979-8-4007-1125-1/25/06
https://doi.org/10.1145/3679240.3734653

Attacks on Ukraine Power Grid. Attacks against Ukrainian electrical companies have been observed in 2015, 2016 and 2022 [8, 10, 34, 47]. These attacks caused a blackout affecting more than twenty thousands citizens in 2015 via the malware called BlackEnergy3 [18], and further disruptions via the malware called Industroyer and Industroyer2 in 2016 and in 2022, respectively [29].

Attack on Energy Sectors in Middle East. The attack targeting the energy and chemical sectors in the Middle East in 2017 [15, 35, 55] was a watershed moment not only in energy system security, but also in industrial control system (ICS) security. The malware named Triton distinguishes itself from other ICS-tailored malware, as it targets a safety instrumented system (SIS), which serves to put a critical infrastructure in a safe state or shut it down to prevent any physical harm. A SIS is considered as the last defense line for critical infrastructures. It is often totally isolated from all other networks and hence hard to reach. Sabotaging a SIS not only causes economical loss for operators, but also directly risks human lives.

Attacks on Western Energy Sector. The "Dragonfly 2.0" campaign starting from 2015 has targeted Western energy sector with sophisticated attacks [51]. The APT actors are seemingly interested in gaining expertise in energy facilities' operation and how to gain access to operational systems, so that they could potentially cause much more serious sabotage. A technical alert regarding this was issued in 2017 [11]. It describes a multistage attack chain, e.g., how APT actors target small networks with weak security first, and then move laterally to bigger networks with more valuable assets within the energy sector. It also indicates that the APT actors were conducting a long-term attack campaign.

Attack on Korea Hydro & Nuclear Power Company. In 2014, a cyberattack on Korea Hydro and Nuclear Power (KHNP) Company, which operates 23 nuclear reactors and provides almost a third of South Korea's energy consumption, prompted a safety drill at nuclear power plants around the country [36]. This attack resulted in a data breach of personal information of ten thousands KHNP employees, documents for at least two reactors, electricity flow charts and radiation exposure estimation for local residents. Although the nuclear control systems themselves have not been evidently compromised, it has raised fears among citizens that such an attack against their critical infrastructure would directly impact their safety.

2.2 APT Capabilities

Building on the examples above, APT actors exhibit the following hallmark capabilities.

Infiltration Abilities. APT actors often utilize a multitude of sophisticated malware and zero-day exploits. Due to weak security of CER products, APT actors can compromise a large number of network-connected devices. General threat actors may use off-the-shelf attack techniques. But APT actors can harness unconventional channels that are hard to defend. In 2024, a series of coordinated explosions targeted pagers and two-way radios used by Hezbollah members in Lebanon and Syria. The blast resulted in at least 37 deaths and over 3,000 injuries. Investigations revealed that Israeli operatives had infiltrated the supply chain by embedding explosives within the devices' batteries before they reached Hezbollah [12]. This operation involved establishing front companies to manufacture and distribute the compromised equipment, exploiting vulnerabilities in global supply chains to deliver weaponized devices to the target group. Other incidents like XZ Utils [25] and SolarWinds [44] showcase infiltration into software libraries or products.

Coordination, Evasion & Persistence. Some of the largest operational botnets are masterminded by APT actors. They are capable of controlling large botnets, planning and coordinating large-scale attacks stealthily. General threat actors lack the level of coordination for large-scale attacks. APTs can also develop sophisticated evasion techniques to circumvent traditional Intrusion Detection Systems (IDS). For instance, by employing adversarial machine learning, APTs can generate malicious payloads to evade detection, allowing for stealthier operations within energy systems.

State Sponsorship. APT actors are more resourceful both technically and financially, often due to state sponsorship. Thus, their missions are commonly related to geopolitics, with the objectives being cyber espionage, interference in foreign countries, political or even societal instability. For instance, APT 28 has reportedly conducted several politically motivated cyberattacks, most notably the 2016 breach and subsequent leak of emails from Hillary Clinton's mailbox [21]. This incident had significant political repercussions, influencing public discourse and media coverage in the 2016 United States presidential election.

Exploiting the Human Factor. Disinformation campaigns can be strategically employed to confuse and mislead security operators during an attack. APTs can execute highly personalized social engineering techniques and phishing attacks, increasing the likelihood of successful breaches. In late 2024, a major cyber espionage campaign compromised multiple U.S. major telecommunications companies including Verizon, AT&T, T-Mobile, and Lumen Technologies. The attackers infiltrated core network components, gaining access to sensitive information of over a million users, including government officials and political figures. Notably, they accessed systems used for court-authorized wiretapping, posing severe risks to national security. The breach remained undetected for up to two years, highlighting vulnerabilities in the nation's critical infrastructure and prompting urgent calls for enhanced cybersecurity measures.

Targeting Critical Infrastructures. APT actors often target critical infrastructures, with the potential to cause damage to society at a rapid speed and wide scale. In 2022, the AcidRain attack significantly disrupted communication systems controlling 5,800 Enercon wind turbines across Germany, endangering approximately 11 GW of power generation capacity. The attack involved the Viasat satellite communication system, where malicious firmware updates rendered 30,000 satellite modems unusable by permanently erasing their access credentials. The intended target of this sophisticated cyberattack was Ukraine, and it has been attributed to the APT 44 (Sandworm) [37].

Leveraging AI & Adaptive Learning. The integration of AI into the offensive strategies of APTs allows the automation of various stages including malware development, reconnaissance, exploitation, and lateral movement, thus shortening the time between the

initiation of an attack and the full compromise of a targeted system [9, 50]. Frontier foundational models can already outperform an average programmer. AI systems enable APTs to execute attack campaigns with increased speed and efficiency, having the potential to automate an entire attack campaign without human intervention. APT attack campaigns can further evolve by using adaptive learning, which refers to the ability to learn from past interactions with defensive measures such as honeypots. This feedback mechanism allows APTs to adapt their strategies, improving their effectiveness despite improved security mechanisms. Consequently, APTs become more resilient, making them increasingly challenging to detect and defend.

3 Attack Paths & Physical Impacts

Decentralized energy infrastructures increasingly integrate Consumer Energy Resources by utilizing solar and wind energy to generate power, buffering energy using battery storage systems, and coordinate large loads like EV charging and heat or cold supply. These residential power systems are interconnected not only through power flow, but also via information flow.

The information flow among devices inside and between these households inevitably makes the entire infrastructure more vulnerable to cyberattacks, and creates a great opportunity for attackers to cause significant impact on individual households and beyond. With the increased complexity of the infrastructure, the number of possible initial access points (IAPs) for attackers surges. In Figure 1, we pinpoint and describe four major IAPs, which grant attackers the access to the most critical cyber assets in decentralized energy systems: the controller of the Consumer Energy Resource.

A direct access to CER controllers can cause, on the one hand, physical impact on the power grid's stability and life of CER equipment, like solar panels and battery cells, or even other electrical home appliances. On the other hand, attackers may use the CER access as a pivot to infiltrate home area networks and compromise other digital devices, e.g., personal computers or IoT devices, for the purpose of stealing sensitive information.

3.1 Gaining Access to CERs

Due to the interconnectedness among devices, the attack flow can often be bidirectional, as shown in Figure 1. For instance, on the one hand, if an attacker has achieved the initial access to the CER devices in home networks, i.e., IAP1, the attacker may further compromise the home router or vendor's cloud infrastructure. On the other hand, if the attacker has obtained the initial access to the home router, i.e., IAP2, or to the vendor's cloud infrastructure, i.e., IAP3, the CERs may be the next devices to be compromised.

In the following, we describe four approaches for gaining access into residential CER devices. While in the first one, the initial access point is the CER device itself, i.e., IAP1, the other three approaches leverage a different initial access point and pivot to the CERs.

IAP1: Firmware-based Approach. Firmware of CERs can contain code carrying vulnerabilities or even acting as a backdoor for a long period of time before being discovered. On the one hand, firmware vulnerabilities may be exploited by attackers, which then grants them some level of control over those involved CER devices. On the other hand, backdoors in firmware may be intentionally or even unintentionally inserted by the developers, which may allow a complete control over CERs. For instance, a backdoor may be created for debugging purposes in the test version of some firmware, but is then mistakenly kept in the released version of the firmware.

However, firmware vulnerabilities and backdoors are not always created by their direct developers, but instead suppliers of some integrated modules inside the firmware. Supply chain attacks have been observed in the past, and have proven to have serious consequences [42]. The access granted by means of firmware vulnerabilities or backdoors either allow attackers to directly interact with the CERs, i.e., command and control, or insert a time or logic bomb containing a series of malicious commands that execute without further interaction with the attackers.

IAP2: Mobile Application-based Approach. CER vendors or third-party monitoring service providers often offer customers a mobile application to interact with their CERs for convenience. Given their popularity, mobile applications have been often targeted by threat actors. The success rate of attackers is boosted by the fact that mobile applications lack security by design, as many application developers do not have adequate security awareness and expertise [43]. Application developers even lack the motivation to design more secure applications, as it does not directly increase their profitability. Mobile applications for energy systems have long been identified as insecure [7]. After compromising the mobile application, an attacker may misinform CER owners to cause negative impact on the load or energy production. Or the attacker may pivot from the mobile device to attack other devices in the system.

IAP3: Botnet-based Approach. The easiest initial access point for attackers is perhaps home routers with weak security and hence vulnerable to botnets. A botnet is a network of infected devices within a command & control infrastructure used for various malicious activities. IoT devices such as home routers have been an easy and attractive target for attackers to form large-scale botnets, which are a powerful amplifying platform for further cyberattacks [6, 28]. For instance, the Mirai botnet [3], as one of the largest botnets in history, has used a simple strategy, i.e., a list of 62 common default usernames and passwords, to gain access primarily to home routers, Internet-connected cameras etc. After gaining access to home routers, devices inside those home networks including CERs may soon fall victim to attackers. Note that a direct disruption on the power grid caused by an IoT botnet has already been proven to be possible [49].

IAP4: Cloud Infrastructure-based Approach. Vendors' cloud infrastructures provide another powerful initial access point for attackers. Owners of residential CERs typically interact with their devices through their vendors' cloud platform. This offers home owners some convenience, as they can remotely monitor and control their CERs from around the world. However, stolen user credentials for cloud platforms that provide monitoring and controlling services for solar energy prosumers are often sold on the dark web [45]. Attackers may collect a large amount of user credentials, and log into the corresponding cloud platforms, and issue malicious commands to a significant number of CERs. Worse yet, vulnerabilities in vendors' cloud platforms may grant attackers the control over an even larger number of CERs, causing more serious impact.

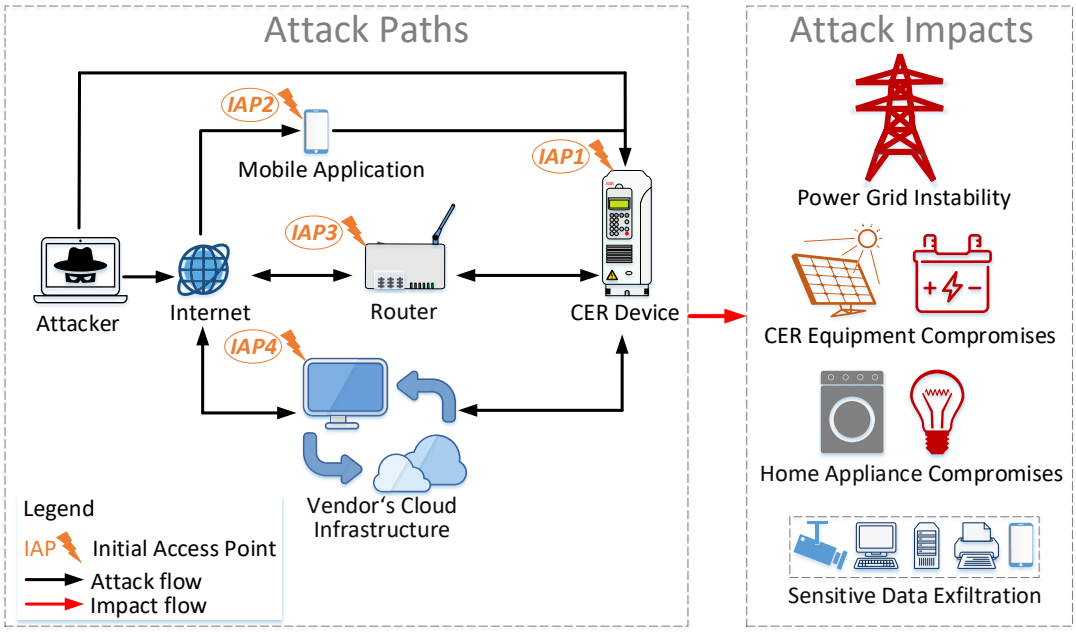


Figure 1: Attack Paths and Potential Attack Impacts.

3.2 Physical Impacts on Energy Systems

The market of solar panels and inverters lacks diversity. More than 80% of inverters shipped worldwide in 2023 are from the top 10 vendors, while the top two vendors account for over 50% of the market [57]. This, however, would make it easier for attackers to cause more serious impacts, in particular on power grid stability, as attackers would need to target only a few inverter vendors. Briefly speaking, as shown in Figure 1, attacks on CERs may lead to power grid instability, CER equipment compromises, home appliance compromises and sensitive data exfiltration. How much physical impact can be achieved depends on the level of privilege an adversary can gain on the Consumer Energy Resources. We describe various privilege levels in the following, starting from the lowest one.

Monitoring API. The lowest privilege level includes an interface for monitoring the device state, energy flows and energy counters of the CER. This is often also provided over the vendor's cloud platform. If an adversary has access to the Monitoring API, there are hardly any direct consequences for the device or the grid. The API may be vulnerable such that the adversary uses the access for privilege escalation. Besides, a denial-of-service attack using the API may have consequences on other services the device provides.

Energy Management API. The next higher level is the interface for the Energy Management System (EMS). The EMS may set operating modes for the CER and setpoints during the operation, e.g., active power limits. The Energy Management API is mostly provided locally as an interface for Energy Management Appliances. Excluding analogue interfaces like Smart Grid ready, we focus on higher level communication interfaces like IEC 61850 or IEEE 1547 (Sunspec Modbus). Especially these high level interfaces allow a plethora of cyberattacks already described in literature:

Load Altering. This describes a coordinated change of active power of a load or generator. This can be done by directly changing the setpoint of the device as described by Li and Yan [31]. Another attack approach is by injecting false data as described by Zhang et al. [58] or practically performed by Müller et al. [39].

Frequency Stability. Frequency can be the target of the Load Altering attack. Most recently explained by Goerke et al. [19] and Dashevskyi et al. [14], a grid frequency deviation of at least 0.2 Hz will start causing cascading effects in grid with protection systems designed for top-down load flow. For an effective attack, how much power can be controlled as well as the speed of the attack is of importance, as the grid has escalating containment reserves in multiple stages and reaction times. The least amount of power is needed to attack the Frequency Containment Reserve. If the attack duration is longer than 30 seconds, the attack has to fight against the automatic Frequency Restoration Reserve and manual Frequency Restoration Reserve additionally.

Voltage Stability. Reduced voltage stability is also an effect of load altering. Targeting the voltage needs less resources than targeting the frequency, but the effect is also limited locally. In addition to altering the active power, reactive power can also be used to impact the voltage as proposed by Hossen et al. [22]. Over-voltage may reduce the lifespan of motor-based devices. Other devices' safety mechanisms may trigger and disconnect from the grid. Naderi et al. [40] proposes an attack scenario where an under-voltage in one distribution grid segment and an over-voltage simultaneously in another segment of the same distribution grid is created. In this scenario, the problem cannot be resolved by changing taps of an on-load tap changing transformer.

Provisioning Interface. The provisioning interface is intended for the installation technicians who initially set up the device. Using

this interface, grid codes, grid support functions and protection functions are modifiable.

Attack Sustainability. The sustainability of an attack is improved if the attacker also has access to the provisioning interface by loosening safety limits above what the local grid code would allow.

Voltage Oscillation. Slow voltage oscillations in the grid are amplified if grid support function parameters of inverters are modified. If inverters control reactive power depending on the voltage, they do so to dampen voltage oscillation. By reversing this function, oscillations are amplified.

Operating System Access. This next higher level of privilege describes the ability of the adversary to execute arbitrary code on the main processing unit of a CER device. That level of access can be gained by exploiting a vulnerability on the device or by updating the firmware to include a backdoor. It is possible to further differentiate between different levels of access in this category; for simplicity, we assume full operating system level access in the present paper.

Escalation to Other Devices. A compromised CER device could be used to attack other devices in the grid. Examples of target devices are smart meters or on-load tap changers [31]. An example is shown by Teymouri et al. [54]. They caused unwanted tap changes through false data on voltage measurements.

Embedded Controller Access. CERs often have a dedicated embedded controller to handle the real-time control tasks. That may include grid protection functions, Pulse-Width Modulation control, or motor control. Some CERs may handle this function on a single CPU, but require a real-time compatible computation stack. Although gaining administrative access to the operating system also enables full access to the embedded controller. It is important to differentiate these two privilege levels, as it leads to different potential physical impacts.

Resonance Attacks. Hossen et al. [22] note that an over-modulated inverter can inject low-order current harmonics. This could lead to distorted voltage at the grid connection point, especially if the state of the grid is that of a weak grid.

4 Countermeasures & Future Directions

A proper defense against attacks on decentralized energy systems requires a collaboration among prosumers, device manufacturers and cloud infrastructure operators. Regulatory agencies should define rules specifying the responsibilities of each party. In the following, we describe several potentially promising defense mechanisms.

4.1 Software-defined Home Networks

Software-defined Networking (SDN) presents a new paradigm for home network security. It enables not only advanced firewall features to block attackers' access to home networks [46], but also microsegmentation to prevent attackers from accessing further devices once inside a home network, and escalating the attack impact [41]. A firewall running as an application on a SDN controller can easily take advantage of the flexibility and programmability of SDN. It monitors incoming and outgoing network traffics, detects and prevents potential attacks, such as horizontal port scans.

Microsegmentation is proposed as a promising solution to reduce the attack surface of home networks [41]. This approach can effectively address botnet-based attack scenarios by enforcing fine-grained network security policies in home networks. First, it creates an asset inventory including all digital home devices and their known vulnerabilities. Then, it uses this information to dynamically allocate those devices, and places them into a number of functional security groups. Further, it isolates the devices using inter- and intra-segment network-level security policies. That is, if any home device is compromised by some malware, this approach aims to prevent the malware from ever reaching the CER device to cause significant impact. This can be extended to a full Zero Trust Architecture where continual verification, least-privilege access, and assume-breach principles to every communication flow.

4.2 Logging & Activity Provenance Tracing

Logging and system activity provenance tracing have developed to be an integral part in the modern secure computing environment [24, 32]. System activity provenance tracing can also go beyond device boundaries, identifying attacks across several devices [33]. As IoT home devices and industrial devices like inverters have rather constrained computing resources, fine-grained logging and system activity provenance tracing are currently not a realistic solution. However, coarse-granular logging and logon activity provenance tracing may strike a right balance between security and resource intensity for these devices.

Logon events can be collected both in local devices including inverters, and in the cloud platforms. These events can record who accessed what devices or which platforms from where. By associating these logon events, i.e., logon activity provenance tracing, security operators can identify normal access patterns. As discussed in Section 3.2, an attacker needs to access numerous devices at the same time to cause significant impact on the power grid. Such access patterns would deviate from those normal access patterns, and should immediately trigger prevention mechanisms.

4.3 Long-term Firmware Support

Many CERs have relatively long life-cycles. For example, battery systems can last for more than 10 years, whereas solar panels can even last for more than 20 years. Providing such a long-term support with respect to firmware is challenging. As more and more consumer energy systems are deployed, there is a significant risk of many becoming obsolete legacy systems without proper firmware maintenance, jeopardizing the security of energy grids, as discussed in Section 3.

One solution is enforce legal compliance requirements like the EU Cyber Resilience Act that call for at least 5 years of support for the "digital components" of a product. Future Network and Information Security directive may also address the compound risk of a large number of CER devices.

Another way to foster firmware maintenance for the whole lifecycle of CER systems is to adopt *open-source development*. Evidently, IoT devices (e.g., wireless routers, security cameras) have benefited significantly from open-source development to strengthen the security, especially after the officially declared end-of-life. It would be tempting to adopt a similar paradigm for CER systems. In fact, there

has been an endeavor to adopt open data formats and protocols for demand response systems, e.g., OpenADR [2]. However, there is a lack of open-source development to the firmware level. While open-source development alone may not be a sufficient solution for the security of CERs, a more open and transparent system architecture for CER systems will certainly be conducive to foster strong long-term community support for legacy CER systems.

4.4 Adequate Contingency Generation

In spite of the uncertainty of energy generation from CERs, modern power grids are already designed to withstand contingency events like a power plant failure or a shortfall of solar energy due to weather conditions. Energy supplies are typically well-provisioned by contingency capacity mechanisms (e.g., by fossil-fuelled generation), such that the grid should be able to provide sufficient energy in the absence of solar or wind energy. If power grids are adequately provisioned with contingency capacity, then the impacts of cyberattacks on CERs will be mitigated by disconnecting susceptible CERs and activating contingency generation.

Recent studies examined the resilience of power grids against cyberattacks on CERs [1, 19, 23, 27, 38], and shows that attackers may compromise CER devices to potentially cause wide-scale destabilization on the power grid via frequency control attacks. Particularly, the study of Hui et al. [23] reveals that power grids are typically designed to cope with inadvertent contingency events, which is insufficient to defend against savvy attackers who may launch concerted attacks. The study simulated the impacts of cyberattacks on smart inverters, which shows that compromising only a low percentage of distributed solar panels is sufficient to trigger wide-scale frequency instability. To effectively utilize contingency generation to counteract the disruptions caused by cyberattacks, we need to address several challenges:

Cost Optimization. A straightforward mitigation strategy is to increase contingency capacity proportional to distributed solar PV generation, which will significantly raise the barrier for attackers. However, increasing contingency capacity will inevitably incur higher costs. Currently, the costs attributed to energy essential services (including contingency generation) contribute to a majority of energy costs. Further increase in contingency capacity will exacerbate the burden of energy consumers. Optimization will be needed to reduce the cost of contingency capacity provision.

Non-local Grid Instabilities. There are other non-local instabilities that cannot be addressed by contingency generation alone. For example, voltage, reactive power and power quality that are caused by local anomalies in the power grid. Such non-local instabilities may cause cascading effects to the grid, requiring more adequate control from the distributors.

5 Conclusion & Open Questions

In this paper, we briefly survey past cyberattacks on energy systems and describe capabilities of APT actors. Then we discuss a few attack paths of these attackers to Consumer Energy Resources in decentralized energy systems, and provide an analysis on what consequences they could have. We present several potentially promising countermeasures.

We conclude this paper with a few open questions.

Question 1: *Should the governments ban insecure CERs?*

Several countries are introducing cyber regulations to ban certain consumer devices (including CERs) that may jeopardize national security [13, 20]. However, the technical justifications, the effectiveness in practice and possible side effects remain largely under-explored. What are the criteria of classifying insecure CERs and the benefits of such measures? How do governments effectively enforce these measures against APTs?

Question 2: *How to improve prosumers' cyber awareness of their CERs?*

Prosumers constitute the largest parts, but also the weakest link, of decentralized energy infrastructures. It is imperative to ensure prosumers' awareness of the cyber threats to energy systems, not just for their own sake, but more importantly for the whole society. What are the tools and policies that can improve prosumers' cyber awareness? How to educate and communicate with prosumers about cyber threats to energy systems?

Question 3: *How should national policies for energy systems adapt in response to the challenges related to APTs' enhanced capabilities using AI?*

Concerns regarding cyber risks associated with AI on energy systems need to be first properly justified, and hence contribute to reasonable national policies. Some concerns are valid, and therefore require immediate regulatory responses. But others may not be reasonable, and may lead to unexpected negative consequences. Policymakers should draft targeted, impactful and effective policies to counter the challenges AI-assisted APTs pose while avoiding unnecessary regulatory burdens to system operators.

Question 4: *How should the responsibility be properly and fairly shared between prosumers, device manufacturers, grid operators, and cloud infrastructure operators?*

Undoubtedly, a collaboration between prosumers, device manufacturers, grid operators and cloud infrastructure operators is indispensable for effectively fending off attacks against decentralized energy systems. The question remains, though, how policymakers can reasonably and fairly distribute the responsibility among these parties, and specify and enforce the penalties in case the responsibility is not properly fulfilled.

Acknowledgements

Sid Chau was funded by Cyber Security Cooperative Research Centre (C11-00306) and CSIRO's Critical Infrastructure Protection and Resilience Mission (R-20215). This work was also supported by the Helmholtz Association under the programs "Energy System Design (ESD)" (topic number 37.12.01) and "Engineering Digital Futures (EDF)" as part of the KASTEL Security Research Labs, Karlsruhe (topic number 46.23.02).

References

[1] Samrat Acharya, Yury Dvorkin, and Ramesh Karri. 2020. Public Plug-in Electric Vehicles + Grid Data: Is a New Cyberattack Vector Viable? *IEEE Transactions on Smart Grid* 11, 6 (2020), 5099 – 5113.

[2] OpenADR Alliance. 2025. OpenADR 3.0. https://www.openadr.org. [Online; accessed 19-Mar-2025].

[3] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou. 2017. Understanding the Mirai Botnet. In *26th USENIX Security Symposium (USENIX Security 17)*. USENIX Association, Vancouver, BC, 1093–1110. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

[4] Australia. 2017. Peak Demand and Energy Forecasts. *Weather* 22 (2017), 4.

[5] D. Bastos, M. Shackleton, and F. El-Moussa. 2018. Internet of Things: A survey of technologies and security risks in smart home and city environments. In *Living in the Internet of Things: Cybersecurity of the IoT - 2018*. 1–7. doi:10.1049/cp.2018.0030

[6] Elisa Bertino and Nayeem Islam. 2017. Botnets and Internet of Things Security. *Computer* 50, 2 (2017), 76–79. doi:10.1109/MC.2017.62

[7] Courtney Bjorlin. 2018. *Many SCADA Mobile Apps Lack Security by Design.* https://www.iotworldtoday.com/security/many-scada-mobile-apps-lack-security-by-design [Online; accessed 26-Mar-2025].

[8] Booz Allen Hamilton. [n. d.]. *WHEN THE LIGHTS WENT OUT.* https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf Accessed: June 2024.

[9] Peter Broklyn, Ralph Shad, and Axel Egon. 2024. The Evolving Thread Landscape Pf Ai-Powered Cyberattacks:A Multi-Faceted Approach to Defense And Mitigate. doi:10.2139/ssrn.4904878

[10] Anton Cherepanov. [n. d.]. *WIN32/INDUSTROYER: A new threat for industrial control systems.* https://web-assets.esetstatic.com/wls/2017/06/Win32_Industroyer.pdf Accessed: June 2024.

[11] CISA. 2018. *Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors.* https://www.cisa.gov/news-events/alerts/2017/10/20/advanced-persistent-threat-activity-targeting-energy-and-other-critical-infrastructure-sectors Accessed: March 2025.

[12] CNN. 2024. *Israel concealed explosives inside batteries of pagers sold to Hezbollah, Lebanese officials say.* https://edition.cnn.com/2024/09/27/middleeast/israel-pager-attack-hezbollah-lebanon-invs-intl/index.html Accessed: March 2025.

[13] European Commission. 2025. EU's Cyber Resilience Act. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act. [Online; accessed 19-Mar-2025].

[14] Stanislav Dashevskyi, Francesco La Spina, and Daniel dos Santos. 2025. *SUN:DOWN - Destabilizing the Grid via Orchestrated Exploitation of Solar Power Systems.* Technical Report. https://www.forescout.com/resources/sun-down-research-report/

[15] Dragos Threat Intelligence. [n. d.]. *CHRYSENE Threat Group Operations.* https://www.dragos.com/threat/chrysene/ Accessed: June 2024.

[16] Ember and Energy Institute. 2024. Share of electricity generated by renewables. https://ourworldindata.org/grapher/share-of-electricity-production-from-renewable-sources?time=2005..latest&country=~OWID_WRL. [Online; accessed 21-Mar-2025].

[17] Ember and Energy Institute. 2024. Share of electricity generated by solar power. https://ourworldindata.org/grapher/share-electricity-solar?tab=chart&time=2005..latest&country=OWID_WRL~DEU~NAM. [Online; accessed 21-Mar-2025].

[18] Marcus Geiger, Jochen Bauer, Michael Masuch, and Jorg Franke. 2020. An Analysis of Black Energy 3, Crashoverride, and Trisis, Three Malware Approaches Targeting Operational Technology Systems. In *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, Vienna, Austria, 1537–1543. doi:10.1109/ETFA46521.2020.9212128

[19] Niklas Goerke, Alexandra Märtz, and Ingmar Baumgart. 2024. Who Controls Your Power Grid? On the Impact of Misdirected Distributed Energy Resources on Grid Stability. In *The 15th ACM International Conference on Future and Sustainable Energy Systems*. ACM, Singapore Singapore, 46–54. doi:10.1145/3632775.3661943

[20] Australian Government. 2024. Australia's Cyber Security Legislative Reforms. https://www.cisc.gov.au/legislation-regulation-and-compliance/cybersecurity-legislative-reforms. [Online; accessed 19-Mar-2025].

[21] Guardian. 2016. *WikiLeaks emails: what they revealed about the Clinton campaign's mechanics.* https://www.theguardian.com/us-news/2016/nov/06/wikileaks-emails-hillary-clinton-campaign-john-podesta Accessed: March 2025.

[22] Tareq Hossen, Mehmetcan Gursoy, and Behrooz Mirafzal. 2022. Self-Protective Inverters Against Malicious Setpoints Using Analytical Reference Models. *IEEE Journal of Emerging and Selected Topics in Industrial Electronics* 3, 4 (Oct. 2022), 871–877. doi:10.1109/JESTIE.2022.3199672

[23] Xiangyu Hui, Samuel Karumba, Sid Chi-Kin Chau, and Mohiuddin Ahmed. 2025. Destabilizing Power Grid and Energy Market by Cyberattacks on Smart Inverters. In *Proc. ACM Intl. Conf. on Future Energy Systems (e-Energy)*.

[24] Muhammad Adil Inam, Yinfang Chen, Akul Goyal, Jason Liu, Jaron Mink, Noor Michael, Sneha Gaur, Adam Bates, and Wajih Ul Hassan. 2023. SoK: History is a Vast Early Warning System: Auditing the Provenance of System Intrusions. 2620–2638.

[25] Sam James. 2025. xz-utils backdoor situation (CVE-2024-3094). https://gist.github.com/thesamesam/223949d5a074ebc3dce9ee78baad9e27

[26] Stamatis Karnouskos. 2011. Stuxnet worm impact on industrial cyber-physical system security. In *IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society*. IEEE, Melbourne, Vic, Australia, 4490–4494. doi:10.1109/IECON.2011.6120048

[27] Samuel Karumba, Sid Chi-Kin Chau, Mohi Ahmed Hammond Pearce, and Helge Janicke. 2024. Systematic Study of Cybersecurity Threats for Smart Inverters. In *Proc. ACM Intl. Conf. on Future Energy Systems (e-Energy) EnergySP workshop*.

[28] Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. 2017. DDoS in the IoT: Mirai and Other Botnets. *Computer* 50, 7 (2017), 80–84. doi:10.1109/MC.2017.201

[29] Pavel Kozak, Ivo Klaban, and Tomáš Šlajs. 2023. Industroyer cyber-attacks on Ukraine's critical infrastructure. In *2023 International Conference on Military Technologies (ICMT)*. IEEE, Brno, Czech Republic, 1–6. doi:10.1109/ICMT58149.2023.10171308

[30] David Kushner. 2013. The Real Story of Stuxnet. *IEEE Spectrum* (Oct. 2013).

[31] Yuanliang Li and Jun Yan. 2023. Cybersecurity of Smart Inverters in the Smart Grid: A Survey. *IEEE Transactions on Power Electronics* 38, 2 (Feb. 2023), 2364–2383. doi:10.1109/TPEL.2022.3206239 Conference Name: IEEE Transactions on Power Electronics.

[32] Qi Liu. 2025. *Cross-Machine Multi-Phase Advanced Persistent Threat Detection and Investigation via Provenance Analytics.* Ph. D. Dissertation. Karlsruher Institut für Technologie (KIT). doi:10.5445/IR/1000179480 37.12.01; LK 01.

[33] Qi Liu, Kaibin Bao, Wajih Ul Hassan, and Veit Hagenmeyer. 2024. HADES: Detecting Active Directory Attacks via Whole Network Provenance Analytics. http://arxiv.org/abs/2407.18858 arXiv:2407.18858 [cs].

[34] Mandiant. [n. d.]. *Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology.* https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/ Accessed: June 2024.

[35] Mandiant. 2017. *New Targeted Attack in the Middle East by APT34.* https://cloud.google.com/blog/topics/threat-intelligence/targeted-attack-in-middle-east-by-apt34/ Accessed: June 2024.

[36] Justin McCurry. 2014. *South Korean nuclear operator hacked amid cyber-attack fears.* https://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack Accessed: March 2025.

[37] Alessandro Mura. 2024. *From technical details to the overall relevance for cybersecurity of critical infrastructures.* Technical Report. https://centri.unibo.it/computational-social-science/it/cosa-facciamo/our-students-papers/mura_cs-cw2024_final.pdf/@@download/file/Mura_CS&CW2024_FINAL.pdf

[38] Ahmed S Musleh, Jawad Ahmed, Nadeem Ahmed, Hunter Xu, Guo Chen, Stephen Kerr, and Sanjay Jha. 2024. Experimental Cybersecurity Evaluation of Distributed Solar Inverters: Vulnerabilities and Impacts On the Australian Grid. *IEEE Transactions on Smart Grid* (2024).

[39] Nils Müller, Kaibin Bao, and Kai Heussen. 2024. Cyber–physical event reasoning for distributed energy resources. *Sustainable Energy, Grids and Networks* 39 (Sept. 2024), 101400. doi:10.1016/j.segan.2024.101400

[40] Ehsan Naderi, Samaneh Pazouki, and Arash Asrari. 2023. A coordinated cyberattack targeting load centers and renewable distributed energy resources for undervoltage/overvoltage in the most vulnerable regions of a modern distribution system. *Sustainable Cities and Society* 88 (Jan. 2023), 104276. doi:10.1016/j.scs.2022.104276

[41] Amr Osman, Armin Wasicek, Stefan Köpsell, and Thorsten Strufe. 2020. Transparent Microsegmentation in Smart Home IoT Networks. In *3rd USENIX Workshop on Hot Topics in Edge Computing (HotEdge 20)*. USENIX Association. https://www.usenix.org/conference/hotedge20/presentation/osman

[42] Pierluigi Paganini. 2021. *SolarWinds hack: the mystery of one of the biggest cyber-attacks ever.* https://cybernews.com/security/solarwinds-hack-the-mystery-of-one-of-the-biggest-cyberattacks-ever/ [Online; accessed 26-Mar-2025].

[43] Brad Ree. 2021. *If IoT devices are being cyber-certified, why aren't mobile applications?* https://www.securitymagazine.com/articles/94445-if-iot-devices-are-being-cyber-certified-why-arent-mobile-applications [Online; accessed 26-Mar-2025].

[44] Mathis Richtmann. 2025. How hackers capture your solar panels and cause grid havoc. https://www.dw.com/en/how-hackers-capture-your-solar-panels-and-cause-grid-havoc/a-71593448/. [Online; accessed 19-Mar-2025].

[45] Secura. 2024. Cybersecurity threats and measures for the solar power sector. https://topsectorenergie.nl/documents/1299/2024-Secura_Report-Cybersecurity_threats_and_measures_for_the_solar_power_sector.pdf.

[46] Sajad Shirali-Shahreza and Yashar Ganjali. 2018. Protecting Home User Devices with an SDN-Based Firewall. *IEEE Transactions on Consumer Electronics* 64, 1 (2018), 92–100. doi:10.1109/TCE.2018.2811261

[47] Joe Slowik. [n. d.]. *Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE*. https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf Accessed: June 2024.
[48] SolarPower Europe. 2024. Global Market Outlook For Solar Power 2024-2028. https://www.solarpowereurope.org/insights/outlooks/global-market-outlook-for-solar-power-2024-2028/detail.
[49] Saleh Soltan, Prateek Mittal, and H. Vincent Poor. 2018. BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid. In *27th USENIX Security Symposium (USENIX Security 18)*. USENIX Association, Baltimore, MD, 15–32. https://www.usenix.org/conference/usenixsecurity18/presentation/soltan
[50] Morgan Stanley. 2024. AI and Cybersecurity: A New Era. https://www.morganstanley.com/articles/ai-cybersecurity-new-era
[51] Symantec. 2017. *Dragonfly: Western energy sector targeted by sophisticated attack group*. https://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack Accessed: March 2025.
[52] Satori Threat Intelligence and Research Team. 2025. Satori Threat Intelligence Disruption: BADBOX 2.0 Targets Consumer Devices with Multiple Fraud Schemes. https://www.humansecurity.com/learn/blog/satori-threat-intelligence-disruption-badbox-2-0/
[53] TechRepublic.com. 2023. Kaspersky's Advanced Persistent Threats Predictions for 2024. https://www.techrepublic.com/article/kaspersky-advanced-threat-predictions-2024/. [Online; accessed 19-Mar-2025].
[54] Armin Teymouri, Ali Mehrizi-Sani, and Chen-Ching Liu. 2018. Cyber Security Risk Assessment of Solar PV Units with Reactive Power Capability. In *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*. IEEE, Washington, DC, 2872–2877. doi:10.1109/IECON.2018.8591583
[55] The MITRE Corporation. [n. d.]. *OilRig*. https://attack.mitre.org/groups/G0049/ Accessed: June 2024.
[56] Wired.com. 2025. A Hacker Group Within Russia's Notorious Sandworm Unit is Breaching Western Networks. https://www.wired.com/story/russia-sandworm-badpilot-cyberattacks-western-countries/. [Online; accessed 19-Mar-2025].
[57] Wood Mackenzie. 2024. Global PV inverter shipments grew by 56% in 2023 to 536 GWac. https://www.woodmac.com/press-releases/2024-press-releases/global-pv-inverter-shipments-grew-by-56-in-2023-to-536-gwac. [Online; accessed 21-Mar-2025].
[58] Jinan Zhang, Qi Li, Jin Ye, and Lulu Guo. 2020. Cyber-physical security framework for Photovoltaic Farms. In *2020 IEEE CyberPELS (CyberPELS)*. IEEE, Miami, FL, USA, 1–7. doi:10.1109/CyberPELS49534.2020.9311533