Advanced Persistent Threat Kill Chain for Cyber-Physical Power Systems

Presekal, Alfan; Stefanov, Alexandru; Rajkumar, Vetrivel Subramaniam; Semertzis, Ioannis; Palensky, Peter

DOI
10.1109/ACCESS.2024.3507386

Publication date
2024

Document Version
Final published version

Published in
IEEE Access

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 9 October 2024, accepted 19 November 2024, date of publication 27 November 2024,
date of current version 9 December 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3507386

RESEARCH ARTICLE

Advanced Persistent Threat Kill Chain for Cyber-Physical Power Systems

ALFAN PRESEKAL, (Member, IEEE), ALEXANDRU ŞTEFANOV, (Member, IEEE), VETRIVEL SUBRAMANIAM RAJKUMAR, (Graduate Student Member, IEEE), IOANNIS SEMERTZIS, (Graduate Student Member, IEEE), AND PETER PALENSKY, (Senior Member, IEEE)
Department of Electrical Sustainable Energy, Delft University of Technology, 2628 CD Delft, The Netherlands

Corresponding author: Alfan Presekal (A.Presekal@tudelft.nl)

This work was supported in part by the European Union (EU) Horizon COCOON Project under Grant 101120221, in part by the Dutch Research Council RESCUE Project under Grant NWO ESI.2019.006, and in part by EU Horizon eFORT Project under Grant 101075665.

ABSTRACT Power systems are undergoing rapid digitalization. This introduces new vulnerabilities and cyber threats in future Cyber-Physical Power Systems (CPPS). Some of the most notable incidents include the cyber attacks on the power grid in Ukraine in 2015, 2016, and 2022, which employed Advanced Persistent Threat (APT) strategies that took several months to reach their objectives and caused power outages. This highlights the urgent need for an in-depth analysis of APTs on CPPS. However, existing frameworks for analyzing cyber attacks, i.e., MITRE ATT&CK ICS and Cyber Kill Chain, have limitations in comprehensively analyzing APTs in CPPS environments. To address this gap, we propose a novel Advanced Cyber-Physical Power System (ACPPS) kill chain framework. The ACPPS kill chain identifies the APT characteristics that are unique to power systems. It defines and examines the cyber-physical APT stages spanning from the initial phases of infiltration to cascading failures and a power system blackout. The proposed ACPPS kill chain is validated with real-world APT attacks on the power grid in Ukraine in 2015 and 2016, and cyber-physical simulations.

INDEX TERMS Advanced persistent threat, anomaly detection, blackout, cascading failures, cyber attack, cyber kill chain, cyber-physical power system, cyber-physical system, cyber security, power grids, power system.

I. INTRODUCTION

Cyber-Physical Power Systems (CPPS) are critical infrastructures undergoing rapid digitalization. Grid digitalization enhances monitoring and control capabilities, as well as intelligence and advanced analytics. Yet, it also introduces new vulnerabilities and cyber threats, which increase the risk of cyber attacks on future CPPS. For instance, some of the most notable incidents include the cyber attacks on the power grid in Ukraine in 2015 and 2016, which employed complex Advanced Persistent Threat (APT) strategies that took several months to reach their objectives and caused power outages. In December 2015, a coordinated cyber attack affected the Ukrainian power grid making it inoperable for several hours [1]. Adversaries initiated the cyber attack from the Information Technology (IT) network segment. The attack began with a spear phishing email campaign directed at power system operators. Using a weaponized Microsoft Excel file enclosed in the phishing emails, adversaries were able to infect the targets with the BlackEnergy3 malware. From there, they established access to the Operational Technology (OT) network controlling the electricity distribution system. In this instance, the cyber attack was not discovered until the attackers took control of the Supervisory Control And Data Acquisition (SCADA) system via remote desktop sessions and disconnected power lines from the grid. The attack caused power outages that affected seven 110 kV and twenty-three 25 kV substations. This incident is acknowledged as

The associate editor coordinating the review of this manuscript and approving it for publication was Pratyasa Bhui.

the first cyber attack in the world to cause a power outage. Adversaries carried out a second attack on Ukraine's power grid in 2016 [2], which resulted in a lower degree of success and impact in comparison to the incident that occurred in 2015. However, the attackers were successful in implementing more sophisticated attack methods using malware by exploiting vulnerabilities in the SCADA communication protocols. In October 2022, Sandworm malware disrupted the OT systems in the Ukrainian power grid, leading to a power outage [3]. These cyber attacks brought attention to the fact that the adversaries possessed a comprehensive understanding of the vulnerabilities present in power system OT networks. This awareness implies they have the potential to inflict even more catastrophic impacts in future attacks. Furthermore, the examples serve to demonstrate the pressing nature of cyber attacks on power systems, necessitating in-depth analysis capabilities of APTs on CPPS and proactive detection and mitigation techniques.

Due to the aforementioned cyber incidents, cyber security research for power grids is gaining more attention. Ideally, cyber attacks on power systems are detected and mitigated in their earliest stages of attack to avoid disastrous outcomes. However, most research is focused on detecting the physical impact of cyber attacks on power systems [4], [5] based on anomalies in physical power system measurements, e.g., False Data Injection (FDI). Detection in CPPS based on the physical impact is only valid in the later stages of a cyber attack. In the initial stages, the majority of attacks operate in cyberspace without affecting the physical system. Consequently, the physical impact-based detection is insufficient, and CPPS must incorporate IT-OT anomaly detection. A study in [6] demonstrates the significance of both cyber and physical components for detecting attacks on Cyber-Physical Systems (CPS). The study examines several cyber attack scenarios, including Denial of Services (DoS) and replay attacks. Nevertheless, the attack scenarios do not correspond to APTs on power grids, e.g., cyber attacks on the Ukrainian power grid in 2015, 2016, and 2022.

The cyber attacks in Ukraine indicate the involvement of APTs in targeting the power grid. APT is a type of complex cyber attack that is orchestrated by well-funded and well-organized adversaries to obtain critical information from its target and inflict damage to the infrastructure [7]. The cyber attacks on the Ukrainian power grid demonstrate the APT's real impact on power systems. However, the existing cyber security framework has not yet covered a thorough investigation of APT stages on CPPS and their consequences on power system operation.

In [8] and [9], the authors use a cyber kill chain framework to analyze the stages of cyber attack in power systems, which was originally proposed in [15]. The cyber kill chain was initially proposed to identify stages of cyber attack in the IT system. Therefore, it does not provide any stages related to the power system. In [10], the stages of cyber attacks in power grids were analyzed using MITRE ATT&CK ICS [17]. In [11], the stages of cyber attacks in power grids were analyzed using SANS ICS [18]. The MITRE ATT&CK ICS and SANS ICS frameworks provide a more comprehensive stage analysis compared to the cyber kill chain. These frameworks incorporate stages that are associated with the physical process of the Industrial Control System (ICS). However, both of them do not include the physical process associated with the power system, i.e., cascading failure and point of no return.

According to our literature review in [7], [12], [13], [15], [16], [17], and [18], there is no framework that provides a comprehensive analysis of APT stages in CPPS. Therefore, in this paper, we provide an in-depth analysis of the capabilities of APTs on CPPS, considering the integration of the IT-OT system and its impact on power system operation. We define the characteristics of APTs on CPPS and propose the first Advanced Cyber-Physical Power System (ACPPS) kill chain framework that defines and examines the cyber-physical APT stages on power grids. It offers comprehensive attack stages for a thorough analysis of APTs on power systems that cause cascading failures and a blackout. Table 1 summarizes the comparison of existing frameworks with ACPPS Kill Chain. This table highlights the novelties of the ACPPS kill chain in comparison to other frameworks. The proposed ACPPS kill chain is validated by cyber attack case studies using cyber-physical simulations in the time domain on the IEEE 39-bus test system.

The cyber attacks in Ukraine indicate the involvement of APTs in targeting the power grid. APT is a type of complex cyber attack that is orchestrated by well-funded and well-organized adversaries to obtain critical information from its target and inflict damage to the infrastructure [7]. The cyber attacks on the Ukrainian power grid demonstrate the APT's real impact on power systems. However, existing research has not yet covered a thorough investigation of APT stages on CPPS and their consequences on power system operation. Several frameworks exist to analyze APT stages in IT systems. Currently, the analysis of cyber attacks on power grids is primarily performed using the cyber kill chain [15], CPS kill chain [16], MITRE ATT&CK ICS [17], and SANS ICS [18]. These frameworks are heavily focused on the cyber stages of the attacks and briefly cover their impact. However, they don't cover the impact of cyber attacks on the operation of the physical system. According to our literature review, there is no framework that provides a comprehensive analysis of APT stages in CPPS, including the integrated IT-OT communication networks and impact on power grid operation, affecting the system stability and causing cascading failures and a blackout. Therefore, in this paper, we provide in-depth analysis capabilities of APTs on CPPS considering the IT-OT system integration and impact on power system operation. We define the characteristics of APTs on CPPS and propose the first Advanced Cyber-Physical Power System (ACPPS) kill chain framework that defines and examines the cyber-physical APT stages on

TABLE 1. Comparison of ACPPS stages with other kill chain frameworks.

Stages	Sub-Stages	[11]	[12]	[13]	[14]	[7]	[8]	[9]	ACPPS Kill Chain
A. Attack Preparation	1. External Reconnaissance	✓	✓	✓	✓	✓	✓	✓	✓
	2. Weaponization	✓	✓	✓	✓	✗	✗	✗	✓
B. Initial Engagement	3. Delivery	✓	✓	✓	✓	✗	✓	✓	✓
	4. Exploit	✓	✓	✓	✓	✗	✗	✗	✓
	5. Privilege Escalation	✗	✗	✓	✗	✗	✗	✗	✓
	6. Credential Access	✗	✗	✓	✗	✗	✗	✗	✓
	7. Defense Evasion	✗	✗	✓	✗	✗	✗	✓	✓
C. Main Attack Phases	8. Establish Foothold	✓	✓	✓	✓	✓	✓	✓	✓
	9. Internal Reconnaissance	✗	✗	✓	✗	✗	✓	✓	✓
	10. Lateral Movement	✗	✗	✓	✗	✓	✓	✓	✓
	11. Collection	✗	✗	✓	✗	✗	✗	✗	✓
	12. Exfiltration	✗	✗	✓	✗	✓	✗	✗	✓
D. Physical System Engagement	13. Inhibit Response Function and Impair Process Control	✗	✓	✓	✗	✗	✗	✗	✓
	14. Unauthorized Control on OT System	✗	✓	✓	✗	✗	✗	✗	✓
E. Power System Impacts	15. Cyber Attack Impacts Power System Operation	✗	✗	✗	✗	✗	✗	✗	✓
	16. Induced Power System Events	✗	✗	✗	✗	✗	✗	✗	✓
	17. Operator and Automated Remedial Action	✗	✗	✗	✗	✗	✗	✗	✓
	18. Slow Cascading Failure	✗	✗	✗	✗	✗	✗	✗	✓
	19. Point of No Return	✗	✗	✗	✗	✗	✗	✗	✓
	20. Fast Cascade and System-Wide Collapse	✗	✗	✗	✗	✗	✗	✗	✓
	21. Blackout	✗	✗	✗	✗	✗	✗	✗	✓
F. Social Impacts and Recovery	22. Social Impacts	✗	✗	✗	✗	✗	✗	✗	✓
	23. OT Recovery and Power System Restoration	✗	✗	✗	✗	✗	✗	✗	✓

power grids. It offers comprehensive attack stages for a thorough analysis of APTs on power systems that cause cascading failures and a blackout. The proposed ACPPS kill chain is validated by cyber attack case studies using cyber-physical simulations in the time domain on the IEEE 39-bus test system.

The key contributions of this paper are as follows:

1) We define the characteristics of APTs on cyber-physical power systems, which are different compared to APTs in IT systems and general CPS.
2) We propose the first ACPPS kill chain framework. ACPPS defines and examines the cyber-physical APT stages on power grids that cause cascading failures and a blackout. This novel kill chain framework offers more comprehensive attack stages for a thorough analysis of APTs on power systems and early-stage mitigation compared to the current frameworks reported in the literature [7], [12], [13], [15], [16], [17], [18].
3) We conduct a comprehensive analysis of how ACPPS kill chain is applied to analyze real-world cyber attacks. The case studies include the actual attacks on the Ukrainian power grids in 2015, 2016, and 2022 based on publicly available information. In addition, an experimental case study is also presented to provide a comprehensive impact analysis in time domain of how cyber attacks on the IEEE 39-bus test system cause cascading failures and a blackout.

The paper is structured as follows. Section I is the introduction. Section II describes the characteristics of APTs on CPPS and compares them with the characteristics of APTs in IT and CPS. Section III proposes the ACPPS kill chain framework, and Section IV provides the case study and experimental results. Section V presents the conclusions of the work.

II. ADVANCED PERSISTENT THREATS ON CYBER-PHYSICAL POWER SYSTEM

A. APT CHARACTERISTICS

The APT terminology was introduced as a name for intrusion activities of APT1 that was discovered by Mandiant in [19]. This intrusion carries out sophisticated and long-term attacks against a variety of targets, including government agencies, defense contractors, and technology companies, primarily in the United States and Canada. The definition of APT has shifted over time to refer to sophisticated adversaries who target critical information with the intention to covertly profit from the stolen information [20].

TABLE 2. Comparison of APT attacks and conventional cyber attacks.

Parameters	APT Attacks	Conventional Cyber Attacks
Actors	Well-organized adversaries	Individual, small group
Attack resources	Resourceful of tools and funding	Limited resources
Motivation	Political, cyber warfare, competition	Financial benefit, hacktivism, personal satisfaction
Target	Governments and enterprise	Mainly individual or organization
Attack technique	Novel/advanced attack techniques	Common attack techniques
Duration	Long term	Single run, short duration
Adaptation	Requires adaptation before final objective	Doesn't require adaptation, objective directly met
Mitigation	Hard to mitigate with security controls	Can be prevented with typical security controls

TABLE 3. Cyber attacks targeting IT system.

Attack Cases	Year	Impacts
Titan Rain [23]	2003	Espionage cyber attack that led to a data breach
Sykipot Attacks [24]	2006	Sykipot malware stealing intellectual property data
Estonia Attack [25]	2007	DDoS attack led to inaccessible official website
GhostNet [26]	2009	Cyber espionage for stealing confidential information
Shadows [27]	2009	Cyber espionage for stealing confidential information
Operation Aurora [28]	2009	Cyber espionage for stealing confidential information
Night Dragon [29]	2009	Cyber espionage for stealing confidential information
APT1 [20]	2013	Cyber espionage for stealing confidential information
Adobe Data Breach [30]	2013	Data breach on 39 million Adobe software users
Yahoo Data Breach [31]	2013	Data breach on 3 billion Yahoo users
Sony Pictures Hacks [32]	2014	Data breach of Sony pictures confidential information
OPM Data Breach [33]	2015	Data breach on US Office of Personal Management (OPM)
Uber Data Breach [34]	2016	Data breach on 57 million Uber users
WannaCry [35]	2017	Ransomware encrypted user data causing the data to be inaccessible
Petya/NotPetya [36]	2017	Ransomware encrypted user data causing the data to be inaccessible
Mariot Data Breach [37]	2018	Data breach on Marriott hotel data
RockYou [38]	2021	Data breach on 8.4 billion passwords

APT implements traditional cyber attack techniques in an organized manner. However, compared to traditional cyber attacks, APT is different. In [21], the authors identify different characteristics among them. Traditional attacks are typically conducted by individuals who are not well organized. The motive for traditional attacks is to obtain financial benefits or personal satisfaction. Meanwhile, in APTs, the adversaries are more well-organized and well-resourced. APTs target specific organizations, e.g., governmental institutions and commercial enterprises. In terms of attack techniques and strategies, APTs are more persistent in establishing a foothold in the target.

The National Institute of Standards and Technology (NIST) identifies three characteristics of APTs [22]. First, APTs pursue their goals in a systematic way over a prolonged period of time. Second, APTs are able to adapt to the efforts that defenders make to endure security control measures. And finally, APTs are determined to establish a foothold and maintain the level of interaction with the targeted system to carry out their final objectives.

In [7], the authors identified three requirements to categorize a cyber attack as an APT. The first requirement is that the attack is hard to prevent, even by implementing multiple security controls. The second is that adversaries must adapt to the targeted system over time. If such adaptability is not necessary for the adversaries, it could mean that the defense system is not properly implemented. For targets with advanced security measures, adaptability will allow adversaries to learn about the targeted system's operation, thereby increasing the likelihood of successful attacks. The third requirement is that the adversary exhibits novel attack techniques not commonly implemented in a typical cyber attack. These requirements clearly distinguish APTs from conventional cyber attacks. With these requirements, it will be hard for individual adversaries to perform such sophisticated attacks. Therefore, in general, APTs are conducted by well-organized adversaries with a considerable number of resources. Table 2 summarizes the comparison of APTs and traditional cyber attacks based on [7], [21], and [22].

B. APTS IN INFORMATION TECHNOLOGY SYSTEMS

IT is a diverse set of technological tools that are used to transmit, store, share, and exchange information. In IT systems, the information is predominantly in the form of digital data. Therefore, APTs in the IT system primarily aim to get access to and exfiltration of digital information. In [20], the author identified that the main objective of the APT attacks is for data exfiltration. Data is a valuable asset for governments and enterprises that potentially can benefit adversaries. Data can be defined as a new form of valuable capital [39]. In [40], the authors identified that data has

TABLE 4. Cyber attacks targeting cyber-physical systems.

Attack Cases	Year	Impacts
Siberian Pipeline [43]	1982	Trojan attack led to Siberian pipeline explosion
Salt River Project [43]	1994	Disruption on water treatment facility
Gazprom [43]	1999	Trojan attack led to disruption of gas flow controller
Maroochy Water System [44]	2000	Unintended release of up to 1 million liters of sewage
CSX Transportation [44]	2003	Worm infection led to disruption in railway signaling system
Slammer worm [44]	2003	Worm disabled safety monitoring in nuclear power plant
Zotob Worm [45]	2005	Disruption of manufacturing SCADA system
Stuxnet Worm [46]	2010	Disruption of controllers in Iranian nuclear reactor facility
Steel Mill [47]	2014	Breakdown of the control system in steel mill
Triton [48]	2017	Adversaries took remote control of industrial control system
Colonial Pipeline [49]	2021	Ransomware disrupted the operation of gas pipeline controllers
Ukraine critical infrastructure [50]	2022	Compromised critical infrastructure including nuclear power plant

TABLE 5. Cyber attacks targeting cyber-physical power systems.

Attack Cases	Year	Impacts
European system operator malware infection [51]	2003	Loss of control in distribution substations for over three days
Aurora experimental cyber attack [52]	2007	Physical damage to power system generator
USB-drive malware in power plant [51]	2012	Three weeks restart delay to power plant
Ukrainian power grid cyber attack 2015 [1]	2015	Power outage affecting 225,000 customers for 6 hours
Ukrainian power grid cyber attack 2016 [2]	2016	200 MW of load was unsupplied
ENTSO-E cyber intrusion [53]	2020	Undisclosed impact
RedEcho malware intrusion [54]	2020	Two hours power outage
ReverseRat malware [55]	2021	Intrusion on power system operator
KA-SAT attack [56]	2022	Disruption on German windfarm satellite communications
Ukrainian power grid cyber attack 2022 [3]	2022	Power outage

social and economic value. Therefore, the exfiltration of sensitive data potentially can lead to social and economic impacts.

APTs typically target the IT systems of organizations or individuals that have access to valuable information or resources. Examples of these types of organizations include government agencies, financial institutions, and large corporations. Table 3 shows an example of APT attacks targeting IT systems. These attacks are potentially carried out by adversaries that are technologically advanced and have access to significant resources, such as actors representing nation-states or organized criminal groups. The impacts of the attacks include data breaches, inaccessible resources, and system operation disturbance. In summary, the impacts of APTs in IT systems lead to digital or cyber impacts and do not directly affect the physical world.

C. APTS IN CYBER-PHYSICAL SYSTEMS

The CPS terminology refers to a system that can interact with humans through a wide variety of components. This system will possess integrated computational and physical functionalities. CPS is able to interact with the physical world and expand its capabilities through computation, communication, and control [41]. In contrast to conventional IT systems, CPSs exhibit distinct characteristics owing to their ability to interface with the physical world through sensors and actuators [42]. Consequently, the CPS also can affect the physical environment through its actuators.

Considering the aforementioned physical properties of CPS, APT attacks on CPS can impact the physical environment. Table 4 summarizes the recorded cyber attacks targeting industrial control systems and their impacts. In general, the impacts can be classified into two categories, i.e., disruption of operation and physical impacts. The differentiation between the impacts of attacks on CPS and IT systems is evident when comparing Tables 3 and 4. Any attack on CPS will not only result in the loss of data, but it also has the potential to lead to disastrous events in the real world, e.g., flooding, explosion, or a blackout.

D. APTS IN CYBER-PHYSICAL POWER SYSTEMS

In addition to the aforementioned attacks on CPS, there are APTs that target CPPS. Table 5 summarizes the attacks on CPPS. In 2003, there was the first reported cyber attack through a malware infection in the SCADA system of a European power grid operator. This caused a loss of energy management-related functionality in several distribution substations for three days [51]. Amongst all the attacks in Table 5, the most notable ones are the cyber attacks in Ukraine in 2015, 2016, and 2022. More detailed discussions on Ukraine's power grid cyber attacks are given in section IV.

As described in Table 5, attacks on CPPS can lead to a physical impact. The impacts of cyber incidents on power system operations are classified into four categories, i.e., (i) impact on physical equipment, (ii) impact on the OT communication network, (iii) impact on energy management

TABLE 6. Comparison of APT attacks in IT Systems, General CPS, and CPPS.

	IT	General CPS	CPPS
Motivation	Financial gain, espionage, or hacktivism	Conflict of interest, cyber war	Conflict of interest, cyber-physical war
Targeted assets	Data	Cyber-physical system process	Power system operation
Attack techniques	Phishing, intrusion, malware-based, or ransomware	Specialized techniques based on industrial control operation	Specialized techniques based on power system operation
Direct impacts	Data loses, data breach	System disruption, physical damage	Disruption, power outage, physical damage
Indirect impacts	Financial loses, reputational damage, political implication	Financial loses, reputational damage, political implication	Financial loses, reputational damage, political implication
Response	Patching vulnerabilities, monitoring network traffic, and restoring data from backups	Combination cyber and physical response	Combination cyber and physical response and need to consider power system state for restoration.

TABLE 7. Impacts Comparison of Attacks in IT System, General CPS, and CPPS.

Categories	Impacts	IT	CPS	CPPS
Digital impact	Application / service disruption	✓	✓	✓
	Communication disruption	✓	✓	✓
	Data loss	✓	✓	✓
	Data breach	✓	✓	✓
Physical impact	Physical operation disruption	✗	✓	✓
	Physical damage	✗	✓	✓
Power system impact	Local power system disruption	✗	✗	✓
	Wide-area power system instability	✗	✗	✓
	Cascading failures	✗	✗	✓
Indirect impact	Financial loss	✓	✓	✓
	Reputation damage	✓	✓	✓
	Political implication	✓	✓	✓

✓: included , ✗: not included

system applications, and iv) impact on data/information [53]. The attacks with an impact in the first category are the most severe cyber-physical system attacks, e.g., [1], [2], [52]. This type of attack can directly cause power outages or damage to insulation, power plants, and transformers. The remaining categories mainly affect the monitoring and control capabilities of the power grid, which may indirectly also result in a blackout. Nevertheless, these non-physical impacts are correlated with the initial phase of cyber attacks, which leads to a more severe impact in later stages. Besides the direct impact on the physical and digital elements in power grids, there is also the risk of complex cascading effects on the power system.

E. APT CHARACTERISTICS IN CYBER-PHYSICAL POWER SYSTEMS

In this subsection, we identify the characteristics of APTs targeting CPPS and compare them with the APTs on IT systems and CPSs. Table 6 summarizes the characteristics of each category. These characteristics are evaluated based on the APT attack cases in the previous subsections. There are six characteristic categories, i.e., motivation, targeted asset, attack techniques, direct and indirect impacts, and responses. In general, a CPPS has similar characteristics as a CPS, with certain notable differences, i.e., attack techniques, impacts, and response. Our proposed criteria are based on the foundation of power system operation.

An advanced attack technique on CPPS was presented in [2] through the SCADA protocol exploit. Although this attack was unsuccessful, other adversaries have already shown their advanced understanding of CPPS operational communication aspects. However, in this attack, adversaries did not show sufficient knowledge of power system operation. Therefore, the impacts of the attack could be mitigated, and the operator could perform immediate system recovery. In the future, adversaries may have substantial knowledge of the power system operation. Instead of only performing reconnaissance on SCADA communication, adversaries may also gather information from power system operations, for example, by obtaining critical information about power system components, load profiles, and physical vulnerabilities of the power grid. Using this information, adversaries can optimize their timing and strategies to maximize the attack impact on power system operation, e.g., cause system instability, cascading failures, and a blackout.

Furthermore, CPPS has more specific impact categories compared to CPS. The comparison of the impact among IT, CPS, and CPPS is summarized in Table 7. We identified three impact levels in CPPS, including local power disruption, wide-area power system instability, and wide-area cascading failure. A local outage happens when a particular power grid element is disconnected from the main grid. In general, this does not affect the main power grid. However, during power system instability, an attack may cause a wide-area power system to become unstable for a relatively short period of time. In this case, there is no significant impact on the power system operation. This impact can be handled through dynamic response from power system operators. Cascading failure impacts occur when the power system cannot recover to its normal operational state. This situation is also indicated by power system instability. However, the remedial actions in the system are not sufficient to tackle this condition. Therefore, the power system will reach a Point of No Return (PNR), followed by cascading failures that lead to a wide-area power outage or even a total blackout [58]. After reaching a PNR, the power system restoration requires considerable time and effort [59]. A more detailed impact of cyber attacks on power systems is discussed in section III.

From the above review, we summarize the following key takeaways from the characteristics of APTs on CPPS:

1) Unlike traditional APTs targeting IT systems, adversaries do not only focus their attention on the cyber components of the CPPS. Adversaries have the potential to target specific components and specific times within power system operation to maximize the impact of their attacks. This can be accomplished by gathering information about critical elements of the power system, power system operational conditions, load profiles, and other relevant information.
2) The impacts on the power system can be further categorized into more detailed and complex stages when compared to those observed in general CPS. These stages include local power outages, power system instability, cascading failures, and a blackout. This classification shows the wider spectrum of attack impact from APTs in CPPS.
3) The restoration process on the power system is complex and cannot be performed by simply restarting the system. The recovery needs to consider many factors, such as black start generation units, load state, generator condition, interconnectors, and the condition of the neighboring power grids. The restoration process for a wide-area power system from a blackout can take several days and even weeks. It is performed incrementally through sequential remedial actions for each electrical substation, power plant, and area/region.

III. ADVANCED CYBER-PHYSICAL POWER SYSTEM KILL CHAIN

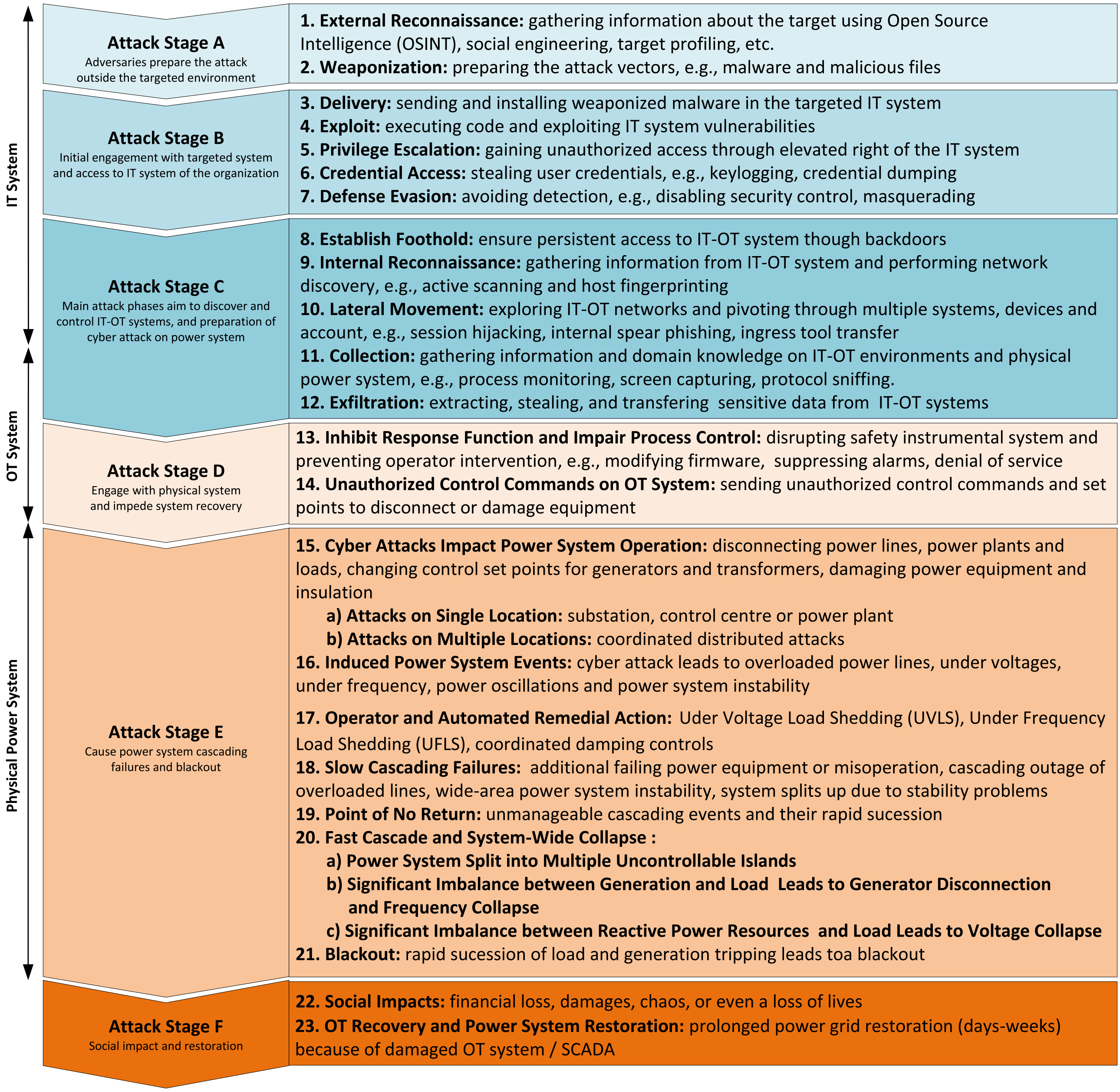
The cyber kill chain is a framework for cyber security investigations and defenses based on intelligence. It is derived from a military model that was initially developed to identify, prepare for the attack, engage, and destroy a target. The cyber kill chain is a method that can be utilized to comprehend better, anticipate, recognize, and fight APTs [15]. The cyber kill chain framework has seven stages, which correspond to the typical phases of a cyber attack. These stages are reconnaissance, weaponization, delivery, exploitation, installation, Command and Control (C2), and actions and objectives. All stages in the cyber kill chain primarily affect the cyber elements of a system and culminate in the action and objective phases. In addition, this framework does not cover the subsequent impact on the physical elements of a system. Consequently, the cyber kill chain framework is inappropriate for identifying APT stages in CPS.

An attempt to cover the physical layer of a cyber-physical system was presented in [16] through the form of a CPS kill chain. This framework is an extension of its predecessor, and it does so by introducing the perturbation of control and physical objectives. However, this framework is lacking in specific stages of the attack and cannot capture the whole process of APT stages. More detailed attack stages on the CPS were proposed by MITRE in [17]. This framework suggested adding three additional categories for the final stages, i.e., impacts, inhibit response function, and inhibit process control. However, within the MITRE framework, the impact part does not cover a comprehensive assessment of the physical system operation in CPPS. Therefore, in this paper, we propose an ACPPS kill chain framework to provide a comprehensive definition and analysis of APT attack stages in CPPS.

Compared to other frameworks, the ACPPS kill chain provides more detailed stages of cyber attacks on power grids. The comparison between the ACPPS stages with other kill chain frameworks is presented in Table 1. We divide the CPPS attack process and impact on power system operation into six stages (A to F). Each attack stage is comprised of a number of sub-stages that are representative of the different attack techniques. Fig. 1 provides a summary of the stages and sub-stages involved in the process. The existing stages of a cyber attack that have been identified in other frameworks [7], [12], [13], [15], [16], [17], [18] are incorporated into the ACPPS kill chain in stages A, B, C, and D, respectively. The ACPPS kill chain proposes new sub-stages for the impact stages in E and F. A detailed step-by-step breakdown of the ACPPS framework development, including theoretical justifications for each stage, is provided in the following subsection. In the following subsection, the summary of all ACPPS kill chain stages is depicted in Fig. 1, and the flowchart illustrates the transitions between stages depicted in Fig. 2.

A. ATTACK PREPARATION

The first stage of a cyber attack is attack preparation. It is during this stage that adversaries are preparing for the attack. The attack preparation stage has two sub-stages, namely external reconnaissance and weaponization. In external reconnaissance, the attacker gathers information about the target system from outside. This information is used to determine target vulnerabilities and strategize the attack on the target. Network scanning, web scraping, social engineering, and other information-gathering tactics are all



Attack Stage A
Adversaries prepare the attack outside the targeted environment

1. External Reconnaissance: gathering information about the target using Open Source Intelligence (OSINT), social engineering, target profiling, etc.
2. Weaponization: preparing the attack vectors, e.g., malware and malicious files

Attack Stage B
Initial engagement with targeted system and access to IT system of the organization

3. Delivery: sending and installing weaponized malware in the targeted IT system
4. Exploit: executing code and exploiting IT system vulnerabilities
5. Privilege Escalation: gaining unauthorized access through elevated right of the IT system
6. Credential Access: stealing user credentials, e.g., keylogging, credential dumping
7. Defense Evasion: avoiding detection, e.g., disabling security control, masquerading

Attack Stage C
Main attack phases aim to discover and control IT-OT systems, and preparation of cyber attack on power system

8. Establish Foothold: ensure persistent access to IT-OT system though backdoors
9. Internal Reconnaissance: gathering information from IT-OT system and performing network discovery, e.g., active scanning and host fingerprinting
10. Lateral Movement: exploring IT-OT networks and pivoting through multiple systems, devices and account, e.g., session hijacking, internal spear phishing, ingress tool transfer
11. Collection: gathering information and domain knowledge on IT-OT environments and physical power system, e.g., process monitoring, screen capturing, protocol sniffing.
12. Exfiltration: extracting, stealing, and transfering sensitive data from IT-OT systems

Attack Stage D
Engage with physical system and impede system recovery

13. Inhibit Response Function and Impair Process Control: disrupting safety instrumental system and preventing operator intervention, e.g., modifying firmware, suppressing alarms, denial of service
14. Unauthorized Control Commands on OT System: sending unauthorized control commands and set points to disconnect or damage equipment

Attack Stage E
Cause power system cascading failures and blackout

15. Cyber Attacks Impact Power System Operation: disconnecting power lines, power plants and loads, changing control set points for generators and transformers, damaging power equipment and insulation
a) Attacks on Single Location: substation, control centre or power plant
b) Attacks on Multiple Locations: coordinated distributed attacks
16. Induced Power System Events: cyber attack leads to overloaded power lines, under voltages, under frequency, power oscillations and power system instability
17. Operator and Automated Remedial Action: Uder Voltage Load Shedding (UVLS), Under Frequency Load Shedding (UFLS), coordinated damping controls
18. Slow Cascading Failures: additional failing power equipment or misoperation, cascading outage of overloaded lines, wide-area power system instability, system splits up due to stability problems
19. Point of No Return: unmanageable cascading events and their rapid sucession
20. Fast Cascade and System-Wide Collapse :
a) Power System Split into Multiple Uncontrollable Islands
b) Significant Imbalance between Generation and Load Leads to Generator Disconnection and Frequency Collapse
c) Significant Imbalance between Reactive Power Resources and Load Leads to Voltage Collapse
21. Blackout: rapid sucession of load and generation tripping leads toa blackout

Attack Stage F
Social impact and restoration

22. Social Impacts: financial loss, damages, chaos, or even a loss of lives
23. OT Recovery and Power System Restoration: prolonged power grid restoration (days-weeks) because of damaged OT system / SCADA

FIGURE 1. Advanced Cyber-Physical power system kill chain framework.

examples of reconnaissance techniques. The external reconnaissance is also associated with Open Source Intelligence (OSINT), where adversaries collect and analyze open-source data related to the target [60]. Initial information gathering is crucial for adversaries to profile the target and determine the next stages of a cyber attack.

The subsequent phase of preparation is weaponization, in which adversaries prepare the tools for a cyber attack. One of the scenarios for weaponization involves software that has been identified in [61] and [62]. The purpose of weaponized software is to enable an attacker to carry out the actions they desire, such as stealing sensitive information, disrupting operations, or taking control of a target system. This purpose is accomplished by transforming the software into malicious software, also known as malware. Another study identified a variant of weaponization, such as weaponization based on artificial intelligence [63], [64]. The weaponized tools that were prepared in the early stage of the cyber attack are utilized in the later stages of the attack.

B. INITIAL ENGAGEMENT AND IT SYSTEM ACCESS

Fig. 1 shows that the second stage in the ACPPS kill chain is the initial attack. It happens when the adversaries perform initial engagement with the targeted system and access the IT system of the organization. In comparison to the previous stage, adversaries in this stage begin to engage

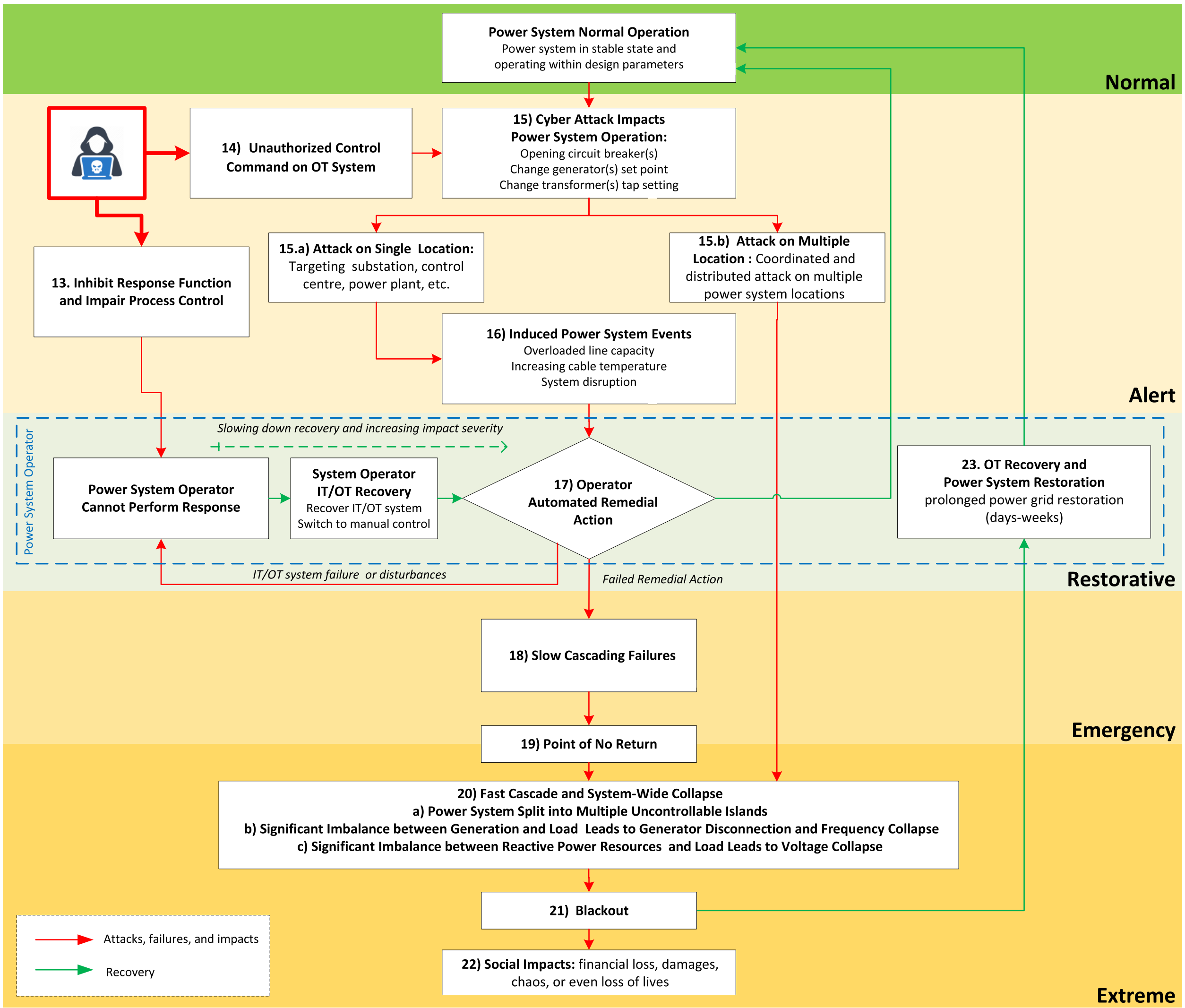

Power System Normal Operation
Power system in stable state and operating within design parameters
Normal
14) Unauthorized Control Command on OT System
15) Cyber Attack Impacts Power System Operation:
Opening circuit breaker(s)
Change generator(s) set point
Change transformer(s) tap setting
13. Inhibit Response Function and Impair Process Control
15.a) Attack on Single Location: Targeting substation, control centre, power plant, etc.
15.b) Attack on Multiple Location : Coordinated and distributed attack on multiple power system locations
16) Induced Power System Events
Overloaded line capacity
Increasing cable temperature
System disruption
Alert
Power System Operator
Slowing down recovery and increasing impact severity
Power System Operator Cannot Perform Response
System Operator IT/OT Recovery
Recover IT/OT system
Switch to manual control
17) Operator Automated Remedial Action
23. OT Recovery and Power System Restoration
prolonged power grid restoration (days-weeks)
IT/OT system failure or disturbances
Failed Remedial Action
Restorative
18) Slow Cascading Failures
Emergency
19) Point of No Return
20) Fast Cascade and System-Wide Collapse
a) Power System Split into Multiple Uncontrollable Islands
b) Significant Imbalance between Generation and Load Leads to Generator Disconnection and Frequency Collapse
c) Significant Imbalance between Reactive Power Resources and Load Leads to Voltage Collapse
21) Blackout
22) Social Impacts: financial loss, damages, chaos, or even loss of lives
Attacks, failures, and impacts
Recovery
Extreme

FIGURE 2. Flowchart representing sequences of APTs on power grids according to the ACPPS kill chain.

and interact with the target that is initiated through delivery. The adversaries prepare the weaponized file and then deliver it to the target. Phishing is the most prevalent technique for cyber attack delivery. The objective of a phishing attack is to convince the victim to open a malicious email or website that delivers the weaponized payload. Phishing attacks frequently employ social engineering techniques to make the message appear legitimate and try to convince the target to click on the malicious link. A phishing attack can be broken down into a variety of different techniques, such as email, clickjacking, cross-site scripting (XSS), drive-by-download, JavaScript obfuscation, and malicious advertisement [65]. Phishing attack primarily focuses on taking advantage of the target's lack of awareness in order to successfully install malicious payloads on the system. This strategy serves as the cyber attack's entry point to infiltrate the targeted system.

Following successful infiltration through the delivery sub-stage, the exploits sub-stage takes advantage of a vulnerability in software, hardware, or a system to execute malicious code and gain unauthorized access. The information on exploits can be obtained from publicly accessible data sources, including the exploit database [66] and the MITRE common vulnerability exposure [67]. An adversary may carry out an exploit with a focus on a zero-day vulnerability in order to increase the likelihood of a successful attack. Zero-day vulnerability is a type of vulnerability that the vendor is either unaware of or has not yet patched [68]. Vulnerability is a crucial component in the process of performing system exploits, as it determines the methodology that is used to carry out the exploit. For example, Ripple20 vulnerability described in CVE-2020 11896 allows for the remote execution of code in SCADA devices [69].

There are two sub-stages that adversaries use to obtain unauthorized authority, i.e., privilege escalation and credential access. Privilege escalation refers to the process of acquiring higher levels of access authority or permissions on a system than those initially granted to the users. This can be accomplished through the use of a variety of methods, such as exploiting software vulnerabilities and hooking. In order to elevate privileges, adversaries exploit software vulnerabilities by taking advantage of a programming error in a program, service, or operating system. Meanwhile, hooking is a technique used by adversaries to take advantage of Application Programming Interface (API) functions, which allows them to elevate privileges and redirect calls for execution. Normally, security permission levels should restrict those malicious activities. Due to privilege escalation, however, adversaries can circumvent these restrictions. Once an attacker has gained access to higher levels of the system, they have a greater chance of being able to perform unauthorized actions, steal sensitive data, or cause damage to the system. Apart from privilege escalation, credential access aims to gain access to a legitimate username, password, or other authentication credentials. Credentials can be retrieved via brute force, password cracking, exploiting vulnerabilities, etc. With privilege escalation and credential access, adversaries can acquire administrative control over a targeted system.

Defense evasion refers to a tactic employed by an adversary to circumvent or undermine security measures in the interest of avoiding detection or analysis. This can be accomplished through a variety of methods, including the obfuscation of malware code, the utilization of encryption in order to conceal malicious traffic, or the manipulation of security tools and monitoring systems. Defense evasion is a core pillar of APTs and other types of sophisticated cyber attacks. Through the use of defense evasion, it is possible for adversaries to go unnoticed by the application of a security system, such as a firewall or an intrusion detection and prevention system.

C. MAIN CYBER ATTACK ON IT-OT SYSTEMS

The aforementioned initial attack phase is followed by the main attack phase, during which the adversaries gain substantial authority to accomplish their objectives. In the main attack stage, the sub-stages involve establishing a foothold, internal reconnaissance, lateral movement, collecting information, command and control settings, and exfiltration.

During the process of establishing a foothold, the adversaries install a backdoor so that they can have persistent and sustained access to the target. Techniques for establishing a foothold include any access or configuration changes made to protect their illegal activity and maintain a foothold on systems. This may involve replacing or hijacking legitimate code, firmware, and other system files, as well as modifying the system's boot process. A backdoor serves as an entry point in a compromised system that enables adversaries to bypass security controls. An adversary with a backdoor can perform internal reconnaissance or discovery on the targeted system. The cyber attack techniques typically implemented in this sub-stage are network sniffing and enumeration, operating system fingerprinting, and remote system discovery. Furthermore, internal reconnaissance gives potential attackers the chance to gather information about the IT-OT system's behavior, such as its network topology, security protection, running applications, and so on, in order to formulate their final attack strategy.

Once an attacker has established a foothold in a network, they may attempt to gain broader access to other components in the IT-OT system. To achieve this objective, adversaries engage in lateral movement sub-stage. In the context of a cyber attack, the term lateral movement refers to the process by which an adversary moves from one compromised system to another within a network. This sub-stage is used by the adversary to pivot to the next point in the environment, thereby positioning themselves closer to the ultimate objective. From lateral movement and internal, adversaries identify the location of the final stage of cyber attack.

During the main stage of the attack, the adversary may conduct information collection and exfiltration. Collection refers to the methods that adversaries employ to obtain domain knowledge from the targeted IT-OT system. The techniques implemented in collection sub-stages are process monitoring, screen capturing, and protocol sniffing. The collection is critical for the planning and execution of attacks in CPPS. Exfiltration is the process of performing an unauthorized transfer of data from a compromised system or network to an external location controlled by adversaries. Meanwhile, information collection aims to obtain valuable information from the system that is being targeted. These two steps have a strong connection to data breaches because they expose valuable information to third parties who are not authorized [70]. This type of attack becomes the ultimate objective of a typical high-profile cyber attack targeting businesses and government institutions. Nevertheless, this type of attack does not cause any direct physical impact.

D. ENGAGEMENT WITH PHYSICAL SYSTEM AND SYSTEM RECOVERY IMPEDIMENT

In stage D, adversaries start to perform direct engagement with a physical system from the OT system. In this stage, adversaries inhibit response functions and impair process control. The first sub-stage aims to impede system recovery before executing the final attack. The potential techniques implemented in this sub-stage are firmware modification, alarm suppression, blocking legitimate communication, data destruction, force system restart or shutdown, and DoS.

Finally, adversaries execute the final stage of the cyber attack through unauthorized control commands on the OT system. In these sub-stages, adversaries are granted the ability to exert control over the system by sending the specified control commands. This attack has the potential to have repercussions for the physical system. For instance, in [52], the Aurora experiment demonstrated how a cyber attack could be used to maliciously control a generator. The experiment demonstrates that a 2 MW synchronous generator can be physically destroyed by malicious control. Another illustration of command and control is the attack on the

Ukrainian power grid, in which the adversaries took control of the SCADA interface and opened circuit breakers for power lines [1]. The command and control stages of cyber attacks rarely happen, but when they do, they have the potential to cause significantly more damage than other types of non-physical cyber attacks.

E. POWER SYSTEM CASCADING FAILURES AND BLACKOUTS

Adverse, unmanaged power system events and disturbances have the potential to result in cascading failures, ultimately leading to the collapse of the entire power grid. The root causes of such events are 1) deterioration and aging of power system equipment, 2) insufficient time to take decisive and adequate corrective actions, and 3) a lack of adequate automated and coordinated controls to take swift and decisive measures [71]. The occurrence of cyber attacks on power grids [1], [2], [3] has raised concerns about the potential for such attacks to instigate the final three root causes mentioned earlier. In [71], the authors comprehensively investigated the analysis of power system impacts caused by single or multiple events. However, cyber attack factors were not incorporated into the events themselves. Therefore, in this subsection, the ACPPS kill chain incorporates an analysis of the possible effects of a cyber attack on the power system. The ACPPS kill chain classifies the impact stages into seven sub-stages, namely (i) cyber attacks impact on power system operations, (ii) induced power system events, (iii) operator and automated remedial actions, (iv) slow cascading failures, (v) point of no return, (vi) fast cascade and power system-wide collapse, and (vii) blackout. Fig. 2 presents a comprehensive overview of the flowchart depicting the various sub-stages involved in assessing the impacts of cyber attacks on the power system.

1) CYBER ATTACKS IMPACT ON POWER SYSTEM OPERATIONS

After adversaries have targeted the physical power system, unauthorized control commands may affect the physical components. The physical effects include but are not limited to, the disconnection of power lines, power plants, and loads, the modification of generator and transformer control set points, and the damage to power equipment and insulation. The disconnection of the power system components can cause widespread power outages and disruptions in the electrical supply. By manipulating the control set points for generators and transformers, adversaries can disrupt the stability and control of the power system, potentially causing voltage and frequency fluctuations. Cyber attacks may involve the destruction of power equipment and insulation. Attacks on critical infrastructure components, such as transformers and generators, can compromise their integrity and result in costly physical damage that necessitates repairs or replacements. Insulation damage can cause faults and short circuits, exacerbating power system disruption.

The cyber attack on power systems may vary with single or multiple targeted locations. Attacks on a single location target a specific facility within the power system infrastructure. For example, an attacker may focus on a substation, control center, or power plant. Meanwhile, attacks on multiple locations are coordinated and distributed attacks that aim to target multiple facilities within the power system simultaneously. The attackers orchestrate a synchronized assault on various points of the infrastructure to maximize the impact and spread the disruption across a wider area. The flowchart of Fig. 2 compares single (15.a) and multiple (15.b) location attacks on the power system. As depicted in Fig. 2, multiple location attacks can directly cause wide-area system collapse.

2) INDUCED POWER SYSTEM EVENTS

The cyber attacks impact on power system operation has the potential to induce subsequent power system events. Initial impacts initiate a chain of undesirable events that disrupt the power system's normal operation and stability. The induced power system events include overloaded power lines, under voltages, under frequency, power oscillations, and power system instability. Overloaded power lines can cause thermal stress, increased line losses, and even transmission infrastructure damage or failure. Under voltages occur when the power system's voltage levels fall below the normal operating range. Under voltages can result in issues such as decreased efficiency of electrical equipment, malfunctioning of sensitive electronic devices, and diminished performance of motors and other loads. Under frequency events refer to instances when the frequency of the Alternating Current (AC) power system drops below the standard operating frequency. Under-frequency conditions can impact power system stability and functionality, and affect the performance of time-sensitive equipment such as motors and generators. Extended under-frequency events can result in cascading failures and widespread power outages if not promptly resolved. Power oscillations are uncontrolled and irregular fluctuations in power flows within a system. The oscillations may cause system destabilization, equipment strain, and voltage and frequency instabilities. Power oscillations can degrade power quality and reliability. Overall, induced power system events resulting from a cyber attack can have severe consequences for the stability, reliability, and safety of the power grid.

3) OPERATOR AND AUTOMATED REMEDIAL ACTIONS

When a power system is subjected to a major disturbance, operator and automated remedial actions are usually undertaken to mitigate the impact of the event. These actions aim to maintain system stability, prevent widespread outages, and minimize the impact of disruptive events. One method of remedial action is Under Voltage Load Shedding (UVLS). When the voltage levels in the power system drop below a certain threshold, UVLS is employed to shed or disconnect certain loads to alleviate the strain on the system. By shedding non-critical loads, UVLS helps to restore and maintain voltage levels within an acceptable range. This action prevents voltage collapse, reduces the risk of equipment damage, and ensures a stable and reliable power supply. Under Frequency Load Shedding (UFLS) is another similar action. In the event of a decrease in the frequency of the power system, UFLS is activated to shed predetermined loads. By shedding certain loads, UFLS reduces the demand on the system, allowing it to recover and stabilize frequency levels. UFLS helps to prevent frequency collapse, maintain system integrity, and avoid widespread power outages. Coordinated damping controls are a set of automated measures employed to dampen power oscillations and stabilize the power system. Power oscillations can occur due to disturbances or imbalances within the grid. Coordinated damping controls utilize various techniques, such as adjusting generator excitation, modifying power system stabilizer settings, or implementing supplementary control signals. These actions aim to counteract power oscillations, enhance system stability, and improve the dynamic response of the power grid. By implementing operator and automated remedial actions such as UVLS, UFLS, and coordinated damping controls, power system operators can respond to critical events or disturbances. Nevertheless, as illustrated in Fig. 2, these corrective measures do not always result in favorable outcomes. Adversaries have the potential to impede remedial action, resulting in elevated undesirable consequences for the power system.

Furthermore, electrical power systems are protected by a variety of automated protection schemes. These protection schemes are implemented on critical components of the power grid, such as generators, transformers, busbars, and power lines. In case of an event such as a short circuit, these schemes aim to isolate the affected component or area on time, thereby safeguarding and ensuring that the equipment will not be stressed or destroyed and the rest of the system will not destabilize. To achieve these goals, a variety of protection schemes are implemented and need to be coordinated. This difficult task is essential as each part of the system needs to be covered by multiple protection schemes. This is done to ensure that multiple operational aspects are addressed, e.g., frequency and voltage protection for generators, and to provide proper coverage in case of maloperation of one device, e.g., distance protection for power lines. Maloperation or improper tuning of the protection relays is also an issue that can occur. Potential maloperation of relays needs to be considered in the protection coordination design. However, as shown in past blackout in North America in 2003 [72], if the settings are not properly tuned, the protection can be triggered to trip power lines and generators.

4) SLOW CASCADING FAILURES

When the remedial action fails, power system events from the previous stage enter the emergency state and lead to slow cascading failure. Cascading failures take place as a consequence of vulnerabilities in interconnected infrastructures [73]. This is a direct consequence of the complex system interactions and interdependencies in electrical power grids. Slow cascading failures are related to additional failing power equipment or maloperation, cascading outage of overloaded lines, wide-area power system instability, system splits up due to stability problems. When there are numerous instances of power equipment failures or operational mistakes within a power system, slow cascading failures may occur. These malfunctions or failures may involve switches, transformers, generators, or other crucial components. Maloperation, such as incorrect settings or human errors in controlling the power system, can also contribute to cascading failures. In the North American blackout mentioned above, the distance protection of power lines was tripped, as the low voltages and overload currents were confused for uncleared fault. This was done as the measured impedance of certain transmission lines fell in Zone 3 of the distance relay. As a result, the disconnection of additional elements led to the continuation of the slow cascading failure propagation. Slow cascading failures can result in the instability of a wide-area power system. This instability refers to a loss of balance between power generation and consumption, which results in voltage and frequency deviations that exceed acceptable limits. In some instances, the instability caused by slow cascading failures can result in the disconnection of power system regions. This occurs when network stability issues become severe enough to cause a separation between network segments. The split can disconnect certain regions from the power supply and disrupt the system's overall operation.

5) POINT OF NO RETURN (PNR)

The power system has the potential to transition from an emergency state to an extreme state, which occurs upon surpassing the PNR. The PNR represents a crucial point in a cascading failure scenario that occurs within a power system. The phenomenon of PNR encompasses a range of intricate and dynamic events including but not limited to 1) the overloading of transmission lines, 2) disconnections of generators, 3) variations in frequency, 4) instabilities in voltage, and 5) loss of synchronism [74]. The propagation of cascading failures is significantly influenced by each of these distinct physical phenomena. At this stage, the situation becomes increasingly difficult to manage, and the sequence of events rapidly accelerates beyond control. After the PNR, the power system enters into a fast cascade and system-wide collapse. In a cascading failure, the power system may divide into uncontrollable islands. This results in system fragmentation and the emergence of isolated regions or islands with an unreliable power supply. The split may result from significant disruptions and failures that impede regular electricity transmission throughout the network.

6) FAST CASCADE AND POWER SYSTEM-WIDE COLLAPSE

A fast cascade is associated with a significant imbalance between the power generation capacity and the power demand in the system. Insufficient generation capacity can cause generator overload, instability, and disconnection from the system due to high demand. The disconnection may lead to an imbalance and subsequent frequency collapse, characterized by a rapid drop in system frequency beyond the acceptable operating range. Fast cascades are also linked to the inability of a stressed power system to maintain its voltage levels in the safety margins. Reactive power is essential for voltage stability in power systems. An imbalance between reactive power resources and demand, as well as limited capability of transferring the necessary reactive power to the loads, can result in voltage collapse in multiple areas of the system. Soon after the fast cascade, a power system suffers a blackout.

7) BLACKOUT

A blackout is a complete and unexpected loss of electrical power over a large area, typically affecting many customers or an entire region. In [75], the authors identified the preliminary stages before the blackout, i.e., the contingency condition, power system problems, protection system trips, and system separation. There are many major power system blackouts happened in the past. For example, the blackout in Italy 2003 [76], North America 2003 [72], Europe 2006 [77], India 2012 [78], Turkey 2015 [79], Ukraine 2015 [1], and United Kingdom 2019 [80]. Those blackouts were triggered by various factors, and only one of them was triggered by a cyber attack. In [74], the authors identified that cyber attacks can accelerate cascading failures and blackouts. Therefore, it is necessary to identify cyber attacks on power grids in the early stage to avoid a blackout and more severe impacts.

F. SOCIAL IMPACTS AND RESTORATION

APTs have the potential to bring a variety of consequences, including economic losses [81]. In addition, cyber attacks on a physical system, i.e., attacks on electrical power grids, potentially can have more severe repercussions. The reason for this is because electrical power grids are considered to be a part of the nation's critical infrastructure. Power system blackouts can lead to wide-area of social consequences, including financial loss, damages, chaos, or even a loss of lives. Power supplies are essential to the functioning of fundamental necessities, such as hospitals, transportation networks, and communication networks [82]. Disruptions of the power grid can have severe consequences for general safety, public health, and the economy. According to research, power outages can have a societal cascading impact, i.e., an increase in the mortality rate [83], disruptions in transportation [84], and an impact on the economy [85]. Furthermore, these indirect impacts have the potential to be politically utilized and become the objective of cyber warfare, as demonstrated by the attack on the Iranian nuclear facility [46] and the conflict between Ukraine and Russia [86].

Upon the culmination of a cyber attack, the system operator endeavors to restore the power system to its normal operational state through OT recovery and power system restoration. The primary objective of OT recovery is to reinstate the OT infrastructure responsible for monitoring and controlling the power system. The process entails the identification and removal of any malicious software, the repair or substitution of compromised hardware, and the reinstatement of the soundness and operability of the OT systems. This process requires a thorough investigation to understand the extent of the attack, the vulnerabilities that were exploited, and the impact on the power system's operational capabilities. Power system restoration involves bringing the entire power system back to its normal functioning state after a blackout. It is a complex optimization problem, which involves advanced coordination across the affected area, as the grid is gradually restored. As power plants are reconnected to the grid, and the loads need to be gradually restored, the communication network plays an important role. In the case of cyber attacks, the validity of the communication system may be compromised. As a result, restoration actions may be further hindered by unresponsive control systems. Due to power system complexity [87], to fully recover the power system requires a complex restoration process within days or weeks. For example, in the North America 2003 blackout that affected 50 million customers, the full restoration process took 48 hours [72]. Another blackout in Italy in 2003 affected 60 million customers and took 12 hours to fully restore the power system [76]. Both of the blackouts were caused by a disruption of the physical power system. The Ukrainian power grids blackout in 2015 was triggered by a cyber attack. This blackout affected 225,000 customers, and took 6 hours to restore the power grids [1]. Additionally, in the Ukrainian power grid attack in 2016, the malware that was utilized contained a module able to launch DoS attack on the IEDs of the targeted substation [2]. Although unsuccessful, the attack aimed to make the IEDs unresponsive to remote commands from the system operators, and could delay the restoration of the affected system.

IV. ADVANCED PERSISTENT THREATS ON POWER GRIDS CASE STUDIES

The digitalization of the electrical power grid has simultaneously introduced the possibility of cyber attacks on electrical power grids as an imminent threat. The repercussions of such sophisticated forms of cyber attack, like the APTs, are to be worried about. They are high-impact, low-frequency events with a wide range of ramifications. It should be noted, however, that only a small number of actual cyber attacks have been recorded as deliberately targeting power grids. However, these attacks have shown that they are capable, and they have given us a glimpse of the potentially disastrous consequences.

In this section, three case studies of cyber attack on power grids, including the real cyber attacks in Ukraine 2015 and 2016, and a hypothetical cyber attack scenario. The analysis of the real cyber attacks is based on the reports in [1], [2], and [3]. Those reports analyzed the stages of cyber attacks in Ukrainian power grids in 2015 and 2016 using the cyber kill chain [15] and SANS Industrial Control System Cyber Kill Chain framework [18]. Compared to the other reports, our survey provides a more detailed cyber attack stage identification and analysis based on the ACPPS kill chain.

In addition to that, we also present a hypothetical cyber attack scenario that was experimented with using a co-simulation testbed of CPPS. The experimental cyber attack is needed because of the limited available information on the physical impact of Ukraine's power grid attacks in 2015 and 2016. Therefore, using the experimental scenarios, we simulate a more detailed physical impact using CPPS co-simulation. To simulate the cyber attack scenarios, we implement CPPS co-simulation, which consists of power system simulation and OT network simulation environment. The power system simulation is implemented using DIgSILENT PowerFactory, and the OT network simulation is implemented using Mininet. Both DIgSILENT PowerFactory and Mininet have been recognized as prominent power system co-simulation tools. These tools have been implemented in many CPPS testbeds for industrial and academic purposes [88]. The DIgSILENT PowerFactory is capable of simulating the power system in real-time using the Root Mean Square (RMS) dynamic model. Meanwhile, the Mininet implements operating-system-level virtualization, which allows the implementation of real communication protocols and cyber attacks. A more detailed discussion of all cyber attack case studies is provided in the following subsection.

A. UKRAINIAN POWER GRID CYBER ATTACK 2015

On December 23, 2015, at 15:30 local time, there was a cyber attack on the Ukrainian power grids. This was the first instance of a cyber attack on power systems that was reported, and it resulted in a power outage. The attackers were successful in compromising three different Distribution System Operators (DSOs) SCADA systems, which allowed them to disconnect a total of seven 110 kV substations and twenty-three 35 kV substations from the distribution network. The attack was successful and resulted in a power outage that impacted a total of 225,000 customers [1].

Fig. 3 depicts the system that governs the operation of power grids. This system includes the IT network, the OT network, and the physical power grids. The IT network is used to assist the operation of the power grid in various ways, including the administration of resources and assets and office operations. From a topological perspective, the IT network is connected to both the Internet and the OT network. On the other hand, they are isolated from one another by means of network segmentation and other forms of security control, such as a firewall. The goal of network segmentations and security controls is to strengthen the network's security measures by separating the different segments of the network. In the OT network, digital substations are responsible for collecting measurement data from the substation bays and station control systems. This data includes the phase angle, active and reactive power, as well as voltage and current magnitude. Afterward, the measurements are transmitted to the control center in order to provide centralized wide-area monitoring. Despite the fact that various cyber security safeguards have been included in the operation of power grids, the cyber attack that happened in 2015 in the Ukrainian power grid highlighted that the system remains vulnerable and can be compromised.

Table 8 gives an overview of the method that was taken during a cyber attack in Ukraine in 2015. Accompanying Table 8, Fig. 3 depicts the locations of the different stages of a cyber attack, each of which is denoted by a number within a red circle. The adversaries apply APT attack strategies to achieve their goals within a few months prior to executing their true objective. The adversaries first gain access to the system through the office network and then go on to the control center and the substations with the intention of triggering a blackout. The majority of the time, the adversary's operations remain undiscovered while operating in a stealthy mode until the last phases of attacks are carried out.

Before launching the attack, in the preparation stage, adversaries gather the profile of the target to prepare spear phishing. Spear phishing is accompanied by substantial information about the target to craft the email and deceive the target. Before sending the phishing, adversaries also prepare malicious Excel files and BlackEnergy3 malware during the weaponization. The attack entered the IT network through spear phishing. The attackers specifically targeted three DSOs while impersonating officials from Ukraine's Ministry of Energy. The malicious emails, which appeared to come from reliable sources, included a weaponized Microsoft Excel file attachment. The attackers used macro vulnerabilities in Microsoft Excel to install malware on the DSO IT network. A macro is a program that uses Visual Basic Application (VBA) scripts to automate tasks in Microsoft Excel. When the recipients enabled the macro, the VBA script was executed, resulting in the installation of BlackEnergy3 malware on the computer.

Following successful installation, the malware established a connection to the attackers' remote C2 server via IP address 5.149.254.114 and port number 80. The malware was specifically designed to communicate to the remote IP address and port number controlled by adversaries. The connection via port 80 appeared to be innocuous. This is due to the fact that port 80 is a commonly used port for website traffic via Hypertext Transfer Protocol (HTTP). Therefore, the attackers could remotely control the BlackEnergy3 malware through its connection to the C2 server.

BlackEnergy3 included some functionalities, i.e., network scanner, file stealer, password stealer, key logger, screenshot capturer, and network discovery. The BlackEnergy3 malware roles were substantial for the initial and main attack stages. The malware discovered information about the IT network

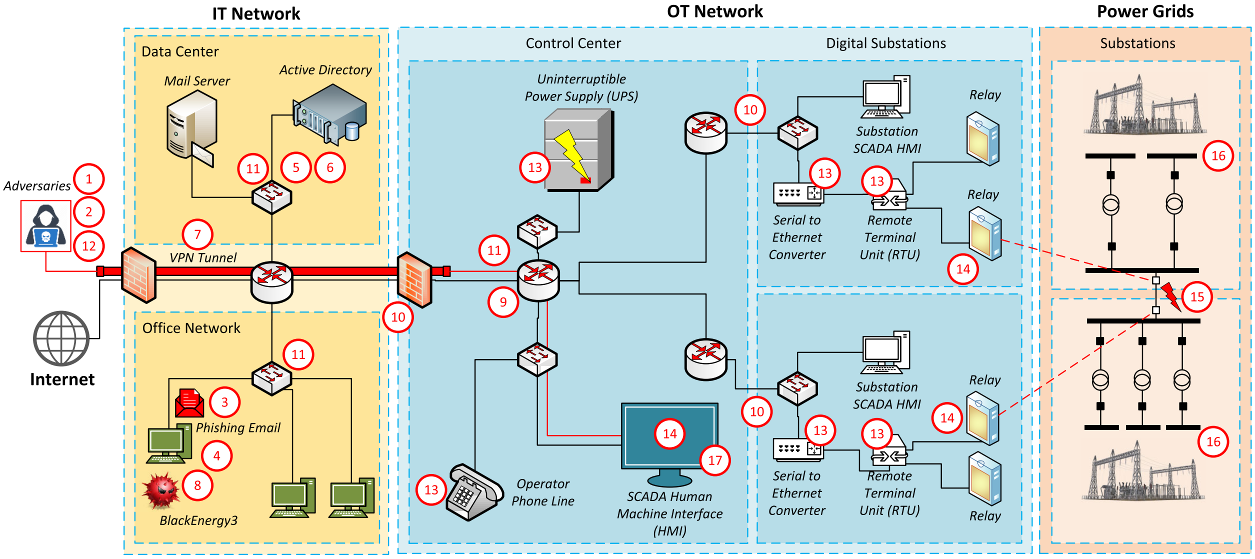


FIGURE 3. Cyber attack on Ukrainian power grids 2015.

TABLE 8. Advanced Cyber-physical system kill chain stages in ukraine cyber attack 2015.

Stages	Sub-stages	Ukrainian power grids cyber attack in 2015 processes
A	1. External Reconnaissance	Target profiling and gathering information about Ukrainian DSOs
	2. Weaponization	Prepare BlackEnergy3 malware and malicious Microsoft Excel files
B	3. Delivery	Send spear phishing email to DSOs operator pretending as an email from Ukraine Ministry of Energy with malicious Microsoft Excel attachment
	4. Exploit	An operator opens the file and exploits Microsoft Excel macro's vulnerability to get remote access
	5. Privilege Escalation	Gain unauthorized access to the database
	6. Credential Access	Get credentials from the active directory
	7. Defense Evasion	Avoid firewall detection through VPN tunnels
C	8. Establish Foothold	Using a backdoor and VPN to maintain its presence
	9. Internal Reconnaissance	Gather information from the OT network system
	10. Lateral Movement	Moving between office network, data center, control center, digital substation
	11. Collection	Collect information from IT and OT systems
	12. Exfiltration	Send the data to the C2 server.
D	13. Inhibit Response Function and Impair Process Control	Telephony denial of service and disable UPS to de-energized control center
	14. Unauthorized Control Commands on OT System	Control SCADA HMI remotely to switch off the breaker
E	15. Cyber Attacks Impact Power System Operation	The breaker on the power grid switched off leading to a power outage
	16. Induced Power System Events	De-energized several substations
	17. Operator and Automated Remedial Action	Operator's initial attempts to recover the power grids failed because of inhibited response function and impaired process control
	18. Slow Cascading Failures	Impact on distribution system operator, did not cause cascading failures and full blackout
	19. Point of No Return	Not applicable
	20. Fast Cascade and System-Wide Collapse	Not applicable
	21. Blackout	Power outages affect 225,000 power grid customers
F	22. Social Impacts	Disruption of energy supply during the winter and financial losses
	23. OT Recovery and Power System Restoration	Operator recovers through manual mode within 6 hours

configuration, such as network segments, network topology, hosts connected, and so on, by using the network scanner and network discovery modules. With BlackEnergy3, attackers could also use a key logger to steal passwords, steal files, and capture screenshots of the targeted computers. This information was critical for preparing the subsequent attack stages. The attackers sent all of the collected data directly to the remote C2 server.

The attackers discovered a vulnerable active directory server during the internal reconnaissance stage, which became a breach point of the IT-OT system. Active Directory (AD) is a database service for IT networked system operations that runs on Windows. An AD manages a user's access permissions by serving as a central authentication and authorization authority for managed accounts, hosts, and services. With centralized authentication and authorization rather than segregated services, AD makes IT system operations easier and more flexible. Active directory databases also store usernames, passwords, and information about hosts and services. As a result, the AD is a critical point for authentication and security. The attackers in the Ukraine 2015 cyber attack compromised the AD server to gain login credentials to the majority of hosts in the IT and OT network. Subsequently, this access is utilized by the adversaries to perform lateral movement through the IT and OT network, including the control center.

After gaining access to the control center, the attackers established a Virtual Private Network (VPN) connection from one of the control center's computers to a remote location on the Internet. VPN enabled the attackers to gain access to the targeted computer via tunnel and encrypted connections. Instead of using a static C2 server with port 80, VPN allowed attackers to access the computer from anywhere on the Internet. Furthermore, the VPN enabled the attackers to avoid detection by firewalls and conceal their true locations. At this point, the attackers had gained complete control and were ready to launch the final attack. The attackers, however, remained undetected, carrying out additional actions to amplify the impact of the cyber attack on the distribution network.

For increasing attack severity, adversaries also impaired legitimate process control and inhibited response function. The impairment of legitimate process control performed through substation device firmware modification wiped out the hard disk and disabled Uninterruptible Power Supply (UPS). The adversaries gained access to substations and compromised Remote Terminal Units (RTUs) and serial-to-Ethernet converters. A serial-to-Ethernet converter connects substation Ethernet communications, e.g., IEC 104, to control center serial communications, e.g., IEC 101. These devices depend on firmware for controlling their processes. The attackers also created malicious firmware and replaced the legitimate firmware in RTUs and serial-to-Ethernet converters, causing them to be inoperable upon reboot. In addition, the malicious firmware prevented grid operators from remotely controlling the substations to perform recovery. KillDisk was used by the attackers to erase hard drives in the control center computers, causing them to be unbootable. KillDisk is a part of BlackEnergy3 malware module that deletes data, registry entries, and system configuration. To prolong the system recovery, adversaries also disabled UPS in the control center, causing them to be inoperative during the blackout. For the inhibit response function, adversaries performed telephony denial of service to make the operator in the control center unable to get information from the outside. After finishing all preparation stages, adversaries launched the final attack on December 23rd by opening the circuit breaker, causing an instant power outage. Cascading impact on the power system was not reported in this attack, but this attack caused a power outage affecting wide area distribution within 6 hours. As a result, the attackers successfully carried out one of the two most advanced cyber attacks on power systems to date.

B. UKRAINIAN POWER GRID CYBER ATTACK 2016

On December 17, 2016, at 23:53 local time, a second cyber attack on Ukraine's power grid took place. This incident was the first publicly reported cyber attack that employed customized malware to target power systems. The malicious software used in the 2016 attack was named CRASHOVERRIDE or Industroyer. The attack had an effect on the SCADA system at the transmission level, and it was directed at a single 330 kV substation as its target. Because of the attack, the distribution network power outage resulted in a total load of 200 MW unable to be supplied. The attack that took place in 2016 was significantly more advanced in terms of its technique than the one that took place in 2015. Fortunately, the damage from this attack was considerably less than the previous one. In [3], an extensive study of this attack is offered and discussed. Within this sub-section, we carried out a review of the attack that took place in 2016 employing the ACPPS kill chain. Table 9 provides a summary of the different stages of the attack according to the ACPPS kill chain. In addition, the study was accompanied by an illustration of the part of the system that was being targeted, which can be found in Fig. 4.

During a few prior months, the adversaries effectively acquired control of the compromised hosts in the control center by utilizing techniques associated with APTs. After that, in the later stages, the adversaries opened circuit breakers and transferred malicious payloads to substations by exploiting SCADA protocol vulnerabilities. On December 17, 2016, at 23:53 local time, these attacks got underway. The attacks were directed at the SCADA system at the transmission level. A single 330 kV/110 kV/10 kV substation was the focus of the attacks, which resulted in an outage at the distribution level. As soon as they became aware of the irregularity in the system, operators reacted swiftly to the attack by switching the controls to manual mode. Fortunately, the operator was able to recover, making this attack ineffective, but it did demonstrate how an advanced protocol exploit might be used to launch an attack.

The overall impact of the cyber assault in 2016 was significantly less due to a number of different factors. The fact that the malicious payload injections did not work properly was the primary cause. It is likely that this was brought about by a manually coded attack technique that did not perform as intended [2]. The attackers should have approached the

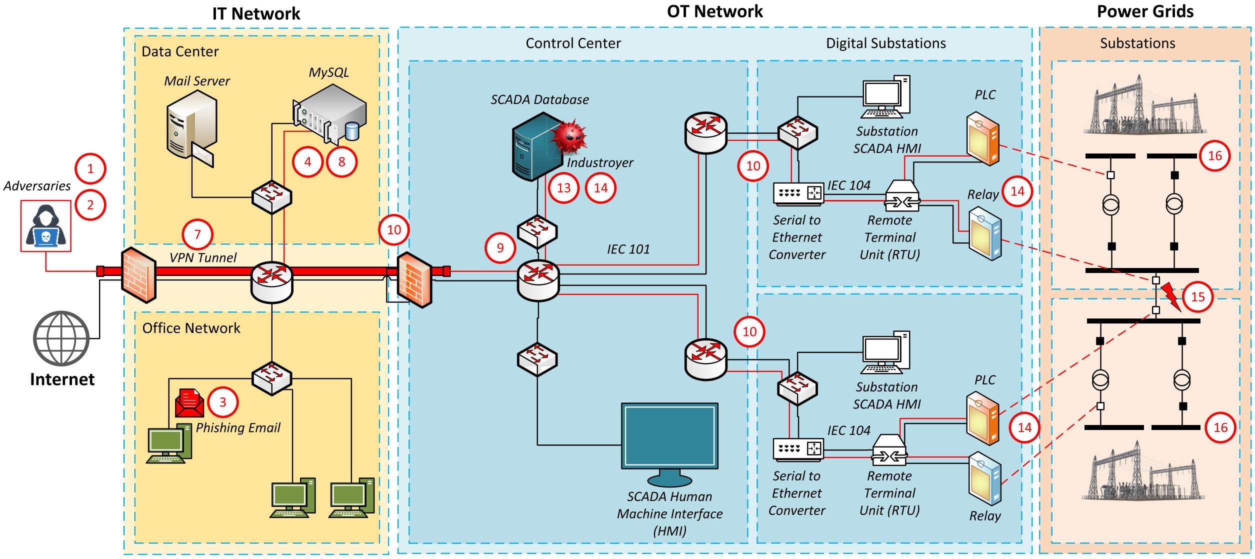


FIGURE 4. Cyber attack on Ukrainian power grids 2016.

TABLE 9. Advanced cyber-physical system kill chain stages in ukraine cyber attack 2016.

Stages	Sub-stages	Ukrainian power grids cyber attack in 2016 processes
A	1. External Reconnaissance	Gather information about the targeted system and identifying potential protocol used in power system operation
	2. Weaponization	Prepare specific malware to exploit specific SCADA protocols, i.e., IEC 101, IEC 104, IEC 61850, and Open Platform Communication (OPC)
B	3. Delivery	Phishing email targeting Ukrainian power grids operator in January 2016
	4. Exploit	Exploit MySQL server vulnerability to gain full control to the server
	5. Privilege Escalation	No information available
	6. Credential Access	No information available
	7. Defense Evasion	VPN tunnel used to bypass the firewall and remotely access the compromised servers
C	8. Establish Foothold	Maintain adversaries presence using compromised MySQL server
	9. Internal Reconnaissance	Malware used to facilitate internal reconnaissance
	10. Lateral Movement	Compromised MySQL server used as pivot point for lateral movement
	11. Collection	No information available
	12. Exfiltration	No information available
D	13. Inhibit Response Function and Impair Process Control	The wiper in CRASSOVERRIDE module removed files relating to ICS operations to prevent instantaneous controller recovery and power system restoration
	14. Unauthorized Control Commands on OT System	Launched the control command attack on December 17, 2016 at 23:53 local time
E	15. Cyber Attacks Impact Power System Operation	The breaker on the power grid switched off lead to power outage
	16. Induced Power System Events	The attacks affected the SCADA system at the transmission level focusing on a single 330 kV / 110 kV / 10 kV substation, resulting in a distribution-level outage
	17. Operator and Automated Remedial Action	No information available
	18. Slow Cascading Failures	Impact on distribution system operator, did not caused cascading failures and full blackout
	19. Point of No Return	Not applicable
	20. Fast Cascade and System-Wide Collapse	Not applicable
	21. Blackout	Power system outage
F	22. Social Impacts	No information available
	23. OT Recovery and Power System Restoration	The disruption was recovered by system operator using manual mode.

development of the protocol payload module in a methodical manner and provided it with the relevant testing environment, such as real SCADA devices. Nevertheless, such instruments are not widely available and are exclusively utilized by operators of industrial systems. As a result, the developed malware failed to operate in its intended function. Yet,

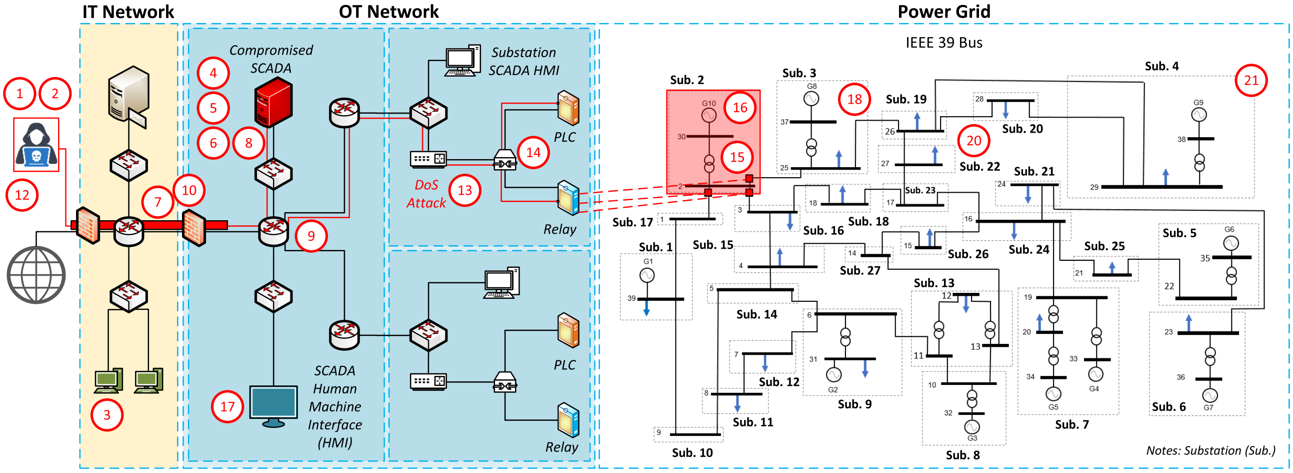


FIGURE 5. Cyber-physical co-simulation experimental setup to analyze the impact of cyber attacks on the power system. The simulated power grid is based on the IEEE 39 bus system with 27 Substations (Sub). The cyber attack impact on power grid started from the malicious opening of the circuit breaker at Bus 2 in Substation 2.

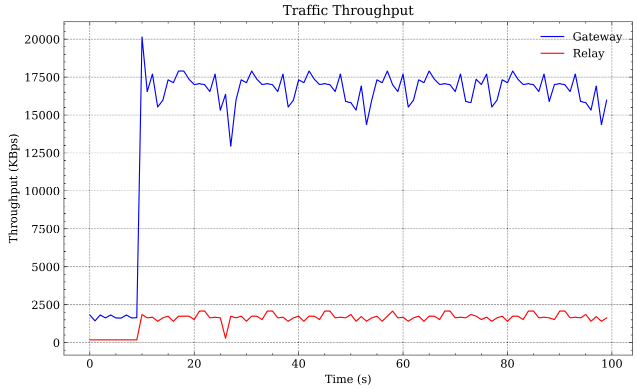


FIGURE 6. Traffic comparison from normal and DoS traffic.

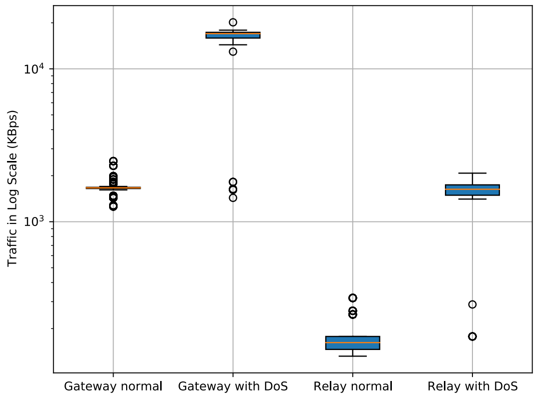


FIGURE 7. Box plot comparison from normal and DoS traffic.

this attack successfully demonstrates a sophisticated APTs with weaponized malware and a deep understanding of the targeted power system. These kinds of attacks have the potential to become more prevalent in the future, which would have a significant adverse impact on the infrastructure of the power grids.

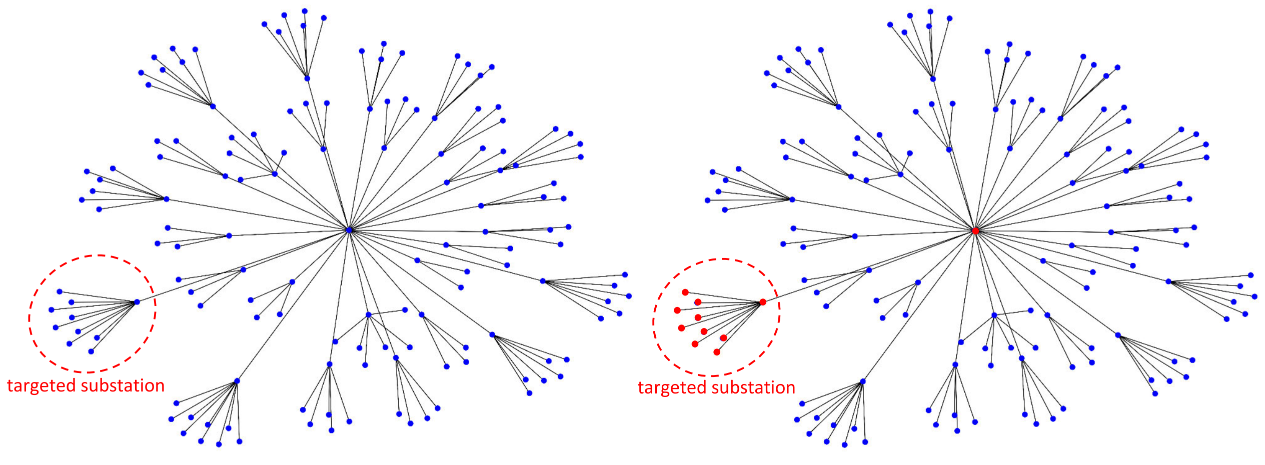
C. UKRAINIAN POWER GRID CYBER ATTACK 2022

In late 2022, a cyber attack targeting the Ukrainian power grids was reported, with evidence pointing to the involvement of the Sandworm hacker group [3]. The adversaries employ the OT-level Living off the Land (LotL) technique, which intends to open the victim's substation circuit breakers, resulting in an unplanned power outage. Compared to the attacks in 2015 and 2016, there is not much information available regarding the attack processes. One reason is that the adversaries employed anti-forensic techniques to hinder the forensic investigation of the attack processes.

The cyber attack started in June 2022 before leading to a disruptive event on October 10 and 12, 2022. There is no available information on how the intruder accessed the OT system. The attack exploits the vulnerabilities of MicroSCADA applications to launch malicious control commands. The malicious control commands successfully open the circuit breakers causing a power outage. However, the detailed impact on the power system is unknown. Based on the available information, the cyber attack process can primarily be categorized using stages C and D of the ACPPS kill chain.

D. EXPERIMENTAL CYBER ATTACK

This subsection discusses an experimental case study involving an example of a transmission grid IT-OT network. The topology of the IT-OT network and the transmission power system is depicted in Fig. 5. The power system is modeled and simulated using DIgSILENT PowerFactory, while the cyber system is emulated through Mininet. It is an open-source network emulator that allows users to create a virtual network topology using software-defined networking (SDN) [89]. Furthermore, it implements operating-system-level virtualization based on the Linux namespace containerization. This allows Mininet to emulate larger communication networks in comparison to typical virtual machines. The emulated



a) Substation under normal operation

b) Substation under DoS attack

FIGURE 8. Graph visualization from attack on substation 2.

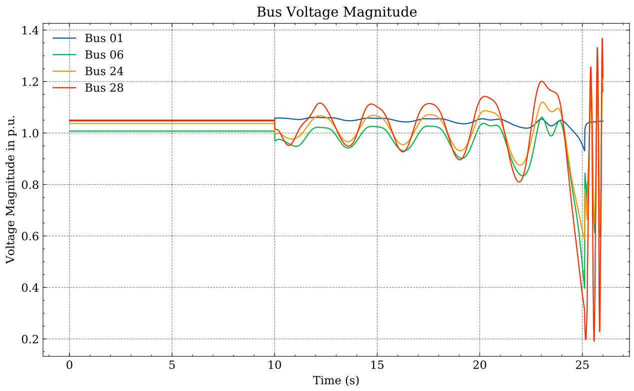


FIGURE 9. Bus voltage magnitude.

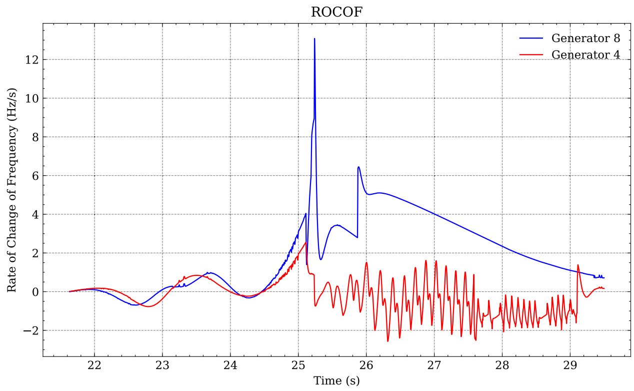


FIGURE 11. Rate of Change of Frequency on Generator Generator 4 and Generator 8.

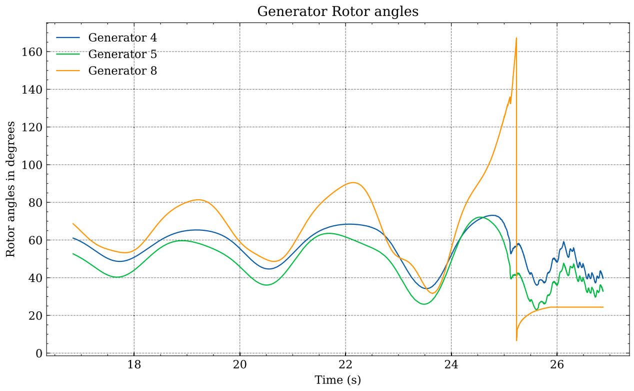


FIGURE 10. Generator rotor angles.

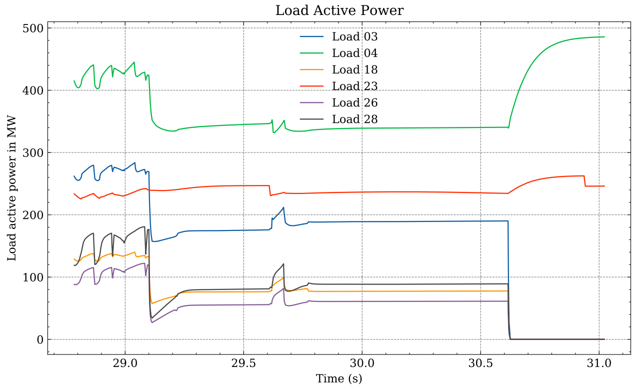


FIGURE 12. Change of load active power for load 03, 04, 18, 23, 26, and 28.

IT-OT network consists of 27 user-defined substations, 118 measurement devices, and over 800 data points for the entire simulated power system. SCADA device functionality within the network is implemented through custom Python scripts.

The simulated power grid runs a Root Mean Square (RMS) simulation of the IEEE 39-bus test system. The power grid simulation provides time-domain measurement data from substation bays, e.g., buses, lines, and generators, in the form of active and reactive power, voltage, and current measurements. All measurement data is then sent from the substation to the control center. The data is also stored in local databases located within substations and the control center.

TABLE 10. Advanced Cyber-physical system kill chain stages in simulated cyber attack.

Stages	Sub-stages	Relation to experimental cyber attack on power grid processes
A	1. External Reconnaissance	Gather information about the targeted system and identify potential communication protocols used in power system operations
	2. Weaponization	Prepare a malicious script based on reverse shell and a payload for the circuit breaker attack
B	3. Delivery	Phishing email targeting grid operator
	4. Exploit	Exploit MySQL server vulnerability to gain full control to the server
	5. Privilege Escalation	Gain admin privilege of SCADA MySQL database
	6. Credential Access	Perform credential theft of username and password accounts from compromised SCADA database
	7. Defense Evasion	VPN tunnel is used to bypass the firewall and remotely access the compromised servers using open source VPN
C	8. Establish Foothold	Maintain presence using compromised MySQL server
	9. Internal Reconnaissance	Perform reconnaissance using publicly available tools, i.e., Nmap, Tshark
	10. Lateral Movement	Compromised MySQL server serves as a pivot point that allows adversaries to compromise other host within the network
	11. Collection	From internal reconnaissance phase, adversaries collect samples of communication packets between control center and substations
	12. Exfiltration	Send the sample protocol to the external remote host
D	13. Inhibit Response Function and Impair Process Control	To prevent the remedial actions, adversaries also launch a DoS attack using hping3 on the OT communication network
	14. Unauthorized Control Commands on OT System	Cyber attack is executed to launch the spoofed payload with open circuit beaker command. The malicious control command open circuit breakers sent in the substation 2
E	15. Cyber Attacks Impact Power System Operation	At time $\tau = 10$ s circuit breaker on lines 01-02, 02-03, and 02-25 maliciously disconnected. Synchronous generator G10 disconnects from the main grid
	16. Induced Power System Events	At τ+7.184 s over frequency protection of synchronous generator G10 trips
	17. Operator and Automated Remedial Action	Operator unable to perform system recovery due to DoS attacks
	18. Slow Cascading Failures	• τ+15.111 to τ+15.233 s : Lines 08-09 and 25-26 in vicinity of attacked substation are tripped by distance protection • τ+15.87 to τ+17.583s : Generators G8 and G9 tripped due to ROCOF interface protection and disconnected. System is now heavily stressed
	19. Point of No Return	Power system enter to critical state and difficult to return to initial condition.
	20. Fast Cascade and System-Wide Collapse	• τ+18.87 to τ+19.072 s : Under frequency load shedding activated. Loads in affected area are shed by 6.7% • τ+19.1 s : Line 16-17 trips on distance protection. This line is the tie-link between two areas. • τ+19.139 to τ+19.879 s : Under frequency load shedding activated. All loads shed by 6.5%.τ+20.621 s : Line 03-04 trips on distance protection. The affected area is completely isolated from the rest of the grid • τ+20.887 to τ+31.941 s : System frequency is still below permissible limits. Under frequency load shedding activated in steps of 5.9% and 7%. The rest of the system stabilizes
	21. Blackout	The attack leads to a partial blackout with 12 busbars being de-energized and a loss of 2285 MW load (37% of total load)
F	22. Social Impacts	The power outage causing disruption on wide area electricity consumer. Consequently, the power outage will disrupt service in various area including healthcare, transportation, communication, etc.
	23. OT Recovery and Power System Restoration	Power system operator need to recover the system using a slower process of manual mode. To recover the OT system, the root cause of cyber attack need to be neutralized

Such a cyber-physical experimental setup allows us to study the impact of cyber attacks on the power system.

In the preparation stage of the attack, the adversaries conduct reconnaissance to gather information about the target, including email addresses, potential operational protocols of the system, etc. This initial information is then used to prepare weaponized cyber attack tools for the later stage of the attack. Subsequently, a weaponized file is then delivered to the target via phishing emails. It serves as an entry point and backdoor for the attackers to the targeted system.

From the entry point, the attackers exploit vulnerabilities in the MySQL SCADA database server in the control

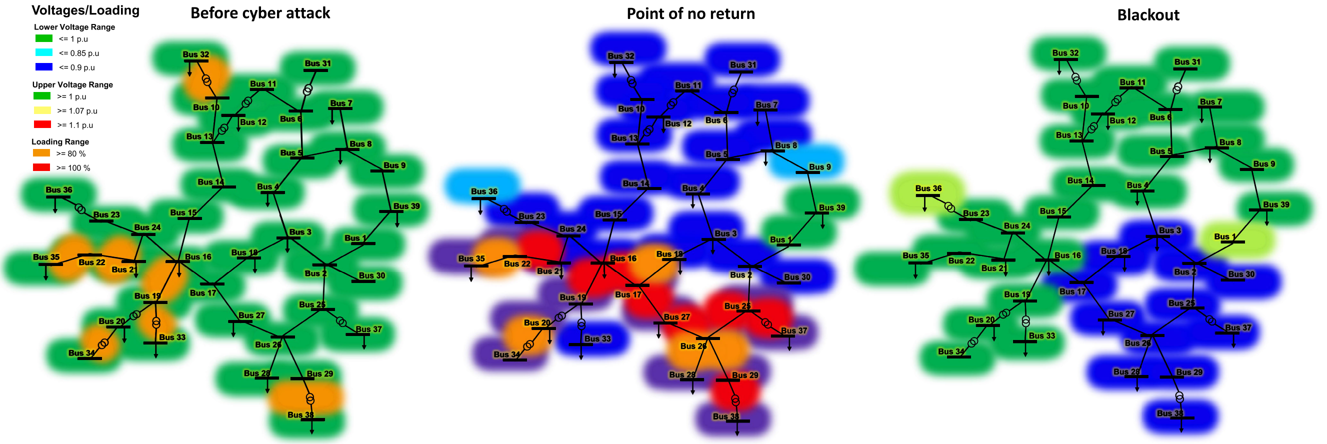


FIGURE 13. Cascading impact visualization.

center. The vulnerability exploit allows the attackers to gain administrator privileges and perform credential system theft. To circumvent firewall detection and secure direct access, attackers enable VPN access from the external network to the compromised MySQL server. Therefore, the compromised MySQL server acts as a central attack location during the main attack stages.

From the compromised MySQL server, attackers maintain their presence and launch the next stages of the attack. This includes internal reconnaissance, lateral movement, data collection, and exfiltration. During these main stages, the attackers learn the operating protocols used for communications between the control center and substations. Through the protocol exploits, the attackers spoof the legitimate control command for opening circuit breakers, as demonstrated in [90]. As shown in Fig. 5, this malicious command subsequently results in the opening of three circuit breakers in substation 2. Under normal circumstances, the system operator would quickly recognize the situation and take immediate corrective action, i.e., the circuit breakers will be closed. In this scenario, however, in addition to the spoofing attack, the attackers also launch a DoS attack against the substation. Fig. 6 shows the traffic comparison in the substation gateway and relay before and after the DoS attack at t=10 s. Before and after the DoS, there is a significant change in substation network traffic. Fig. 7 depicts a statistical summary of the traffic data, including the minimum, median, maximum, first quartile, and third quartile. The box plot also indicates the variability, spread, and skewness of the data. Meanwhile, the circles in the plot indicate the outlier data. Furthermore, the attack location is visualized in Fig.8. In graph-based visualization, red nodes represent the anomalous traffic due to DoS traffic, and blue nodes represent the normal ones. This graph-based anomaly visualization is presented based on our previous research in [92]. Due to the DoS attack, timely corrective actions are made more difficult because commands sent from the control center do not reach the substation in a timely manner. As a result, system stability is affected, leading to cascading failures and a power outage. Table 10 summarizes the simulated cyber attack stages based on the ACPPS kill chain.

The aforementioned cyber attack leads to the malicious disconnection of lines 01-02, 02-03, and 02-25, as well as a DoS attack that inhibits the system operator's capacity to carry out remedial measures. Consequently, the prolonged cyber attack affects the stability of the power system. After this cyber-induced contingency, the system becomes unstable due to the loss of three transmission lines and the resulting disconnection of a major generating unit. As can be shown in Fig. 9, for a prolonged period after the attack, the system is intact, but due to the imbalance between generation and consumption, voltage instability occurs. This can be seen by the oscillations in the voltage magnitudes measured in the buses of the system. Due to this imbalance and the limited capacity of the transmission lines in the vicinity of the attack location to support the power flows, multiple lines are disconnected by distance relays operating on sustained under voltages and over currents. A similar phenomenon was also observed during the 2003 cascading failures and blackouts in North America [91]. A critical line tripped because of incorrect operation of zone 3 distance protection, which exacerbated the domino effect, contributed to the spread of the cascading phenomenon, and ultimately resulted in a widespread power outage [72].

As a result of multiple line disconnections, oscillations are observed between the generators in the affected area and the rest of the system. This is observed in Fig. 10, where it can be seen that generator 08 is oscillating against generators 04 and 05. The resulting instability and the absence of remedial actions cause two generators, namely G8 and G9, to be tripped by their interface protection due to the high Rate of Change of Frequency (ROCOF) condition. As seen in Fig. 13, generator 08 is exceeding the ROCOF setting of 2 Hz/s for over 500 milliseconds, which is the protection setting. Now, due to the loss of generation, system frequency

TABLE 11. Summary of ACCPS Kill Chain Implementation for Real Cyber Attack in Ukraine 2015 and 2016, and Experimental Cyber attacks.

ACPPS Kill Chain		Ukraine 2015	Ukraine 2016	Experimental Attack
Stages	Sub-Stages			
A. Attack Preparation	1. External Reconnaissance	✓	✓	✓
	2. Weaponization	✓	✓	✓
B. Initial Engagement	3. Delivery	✓	✓	✓
	4. Exploit	✓	✓	✓
	5. Privilege Escalation	✓	NA	✓
	6. Credential Access	✓	NA	✓
	7. Defense Evasion	✓	✓	✓
C. Main Attack Phases	8. Establish Foothold	✓	✓	✓
	9. Internal Reconnaissance	✓	✓	✓
	10. Lateral Movement	✓	✓	✓
	11. Collection	✓	✓	✓
	12. Exfiltration	✓	✓	✓
D. Physical System Engagement	13. Inhibit Response Function and Impair Process Control	✓	✓	✓
	14. Unauthorized Control on OT System	✓	✓	✓
E. Power System Impacts	15. Cyber Attack Impacts Power System Operation	✓	✓	✓
	16. Induced Power System Events	✓	✓	✓
	17. Operator and Automated Remedial Action	✓	✓	✓
	18. Slow Cascading Failure	✓	✓	✓
	19. Point of No Return	NA	NA	✓
	20. Fast Cascade and System-Wide Collapse	NA	NA	✓
	21. Blackout	✓	✓	✓
F. Social Impacts and Recovery	22. Social Impacts	✓	NA	✓
	23. OT Recovery and Power System Restoration	✓	✓	✓

✓ = Available; NA = Not Available

TABLE 12. Comparison of ACCPS Kill with Other Frameworks for Cyber Attack Stages Identification.

Frameworks	Number of Stages			Total All Stages
	IT/OT	Physical	Secondary Impact and Recovery	
Cyber Kill Chain [11]	7	0	0	7
CPS Kill Chain [12]	5	2	0	7
MITRE ATT&CK ICS [13]	12	2	0	14
SANS ICS [14]	5	0	0	5
ACPPS Kill Chain	12	9	2	23

starts plummeting, and emergency load shedding is activated to preserve system integrity. This is illustrated in Fig 12. Ultimately, the cyber attack led to a partial blackout with 12 busbars being de-energized and a loss of load amounting to 2285 MW. In Figs. 9-12, cyber attack action that opens the breaker executed at time $\tau = 10$ s. The impacts of cyber attacks are shown after τ.

The entire power system comparison before and after the cyber attack and the propagation of cascading events are shown in Fig 13. The left image shows the heatmap of the voltage magnitudes and lines loading before the cyber attack simulation (τ-1 s), while the right depicts the outcome after the cyber attack (τ+50 s). The middle image depicts the state of the system at the point of no return. As it can be seen, most of the system is stressed, with very low voltage levels and overloaded transmission lines. From the simulated cyber attack, although it was only executed from a single compromised substation, the impact of the attack is not local. This simulation shows that cyber attacks on power grids can cause wide-area cascading impacts.

E. RESULT AND DISCUSSION

Based on the aforementioned cyber attack case studies, the ACPPS kill chain is able to identify all stages of cyber attacks in power grids. Table 11 summarizes all case studies mapping into all stages of the ACPPS kill chain. ACPPS kill chain can identify more granular stages of cyber attacks. In the Ukraine 2015 and 2016 case studies, the ACPPS kill chain was unable to identify some stages. The reason is that there is no available information associated with the particular stages. For example, neither real case of a cyber attack provided any information related to the cascading failure or point of no return. These stages required information related to the power system measurement, and the available reports in [1], [2], and [3] only provided information related to the impact on IT and OT systems. In the experimental attack, we are able to capture power system measurement data from the co-simulation. Therefore, the experimental case study provides a more comprehensive analysis of cyber attacks and their impact on the CPPS.

Compared to other cyber attack stage identification frameworks, the ACPPS kill chain provides more detailed stages. Table 12 summarizes the comparison of the ACPPS kill chain with other frameworks. The ACPPS kill chain refers to the MITRE ATT&CK ICS framework as the most comprehensive cyber attack stage identification for the IT and OT systems. Therefore, from the stages in the IT/OT network, the ACPPS kill chain provides the same quantity of stages as the MITRE ATT&CK ICS. During the physical stages, the ACPPS kill chain proposed seven new stages associated with the cyber attack's impact on the power system. The ACPSS kill chain also proposed new stages associated with secondary impact and recovery. Overall, there are 23 stages in the ACPPS kill chain, which provides nine new stages that are unavailable in other frameworks. Therefore, by enhancing the granularity of cyber attack stages by a factor of 0.64, the ACPPS kill chain improves the effectiveness of identifying cyber attack stages in CPPS.

Despite providing a more detailed stage analysis of cyber attacks on CPPS, the ACPPS kill chain remains inadequate in identifying all stages of an attack, primarily due to the absence of power system data, as indicated in Table 11. A significant factor contributing to this limitation is the insufficient integration among IT, OT, and physical power systems. The lack of seamless integration creates silos that hinder comprehensive monitoring and analysis. Fortunately, the ongoing digitalization of power systems presents a promising solution to this problem. The convergence of IT, OT, and physical power systems through digitalization facilitates real-time data sharing and interoperability, which are crucial for holistic situational awareness and more effective threat detection. This integration not only promises to fill existing data gaps but also provides a unified platform for implementing advanced security measures that can preemptively identify and mitigate sophisticated cyber threats. Consequently, the ACPPS kill chain could be refined into an innovative framework for analyzing cyber attacks on CPPS, providing a more comprehensive representation of the attack stages.

The current version of the ACPPS kill chain only provides the stages of cyber attack in CPPS and does not quantitively assess every stage of the attack. For future work, it is possible to provide quantitative stages identification on the ACPPS kill chain. One potential solution is to integrate AI with the ACPPS kill chain. This is aligned with the state-of-the-art AI application for cyber security applications [93], [94], [95], [96]. With the comprehensive quantitative matrices and AI application, the ACPPS kill chain can be used to classify anomalous events into specific stages in the ACPPS kill chain. Furthermore, it is also possible to predict the potential impact of cyber attacks on power systems to avoid severe impacts.

V. CONCLUSION AND RECOMMENDATIONS

In this research, APTs to CPPS were investigated. This research presents three parts of contributions.

In the first part, the paper identified and compared the characteristics of APT attacks in IT, CPS, and CPPS. We define the characteristics of APTs on CPPS, which are different compared to APTs in IT systems and general CPS.

In the second part, we propose a novel ACPPS kill chain framework. ACPPS defines and examines the cyber-physical APT stages on power grids that cause cascading failures and a blackout. This novel kill chain framework offers more comprehensive attack stages for a thorough analysis of APTs on power systems and early-stage mitigation compared to the current frameworks reported in the literature.

In the third part, this manuscript provides an in-depth analysis of actual and experimental cyber attacks on power grids. The in-depth analysis is performed based on the proposed ACPPS kill chain on Ukraine's 2015, 2016, and 2022 cyber attacks and experimental scenarios.

Overall, this manuscript's contribution is by enhancing state-of-the-art research comprehension of APTs targeting CPPS. It achieves this by introducing a novel framework of ACPPS kill chain for analyzing these threats and providing practical insights through both real-world and experimental case studies. Through these contributions, this work aims to stimulate further research and development endeavors focused on improving the resilience of CPPS in response to evolving cyber threats. It is important to note that we are currently living in a world where artificial intelligence plays an increasing role. Therefore, there is an opportunity for future research on integrating AI with the ACPPS kill chain. The ACPPS kill chain navigates the stages of cyber attacks in CPPS while the AI helps to classify anomalous events into the associated ACPPS kill chain stages. This integration will provide a comprehensive solution for cyber attack mitigation in the earlier stage of the ACPPS kill chain and prevent more severe impacts. In addition, in the current version, the ACPPS kill chain does not provide quantitative metrics to evaluate APTs in CPPS. With AI integration, the ACPPS can provide more comprehensive quantitative evaluation metrics to predict and mitigate cascading failures and points of no return.

REFERENCES

[1] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies," in *Proc. 70th Annu. Conf. Protective Relay Engineers (CPRE)*, College Station, TX, USA, Apr. 2017, pp. 1–8.

[2] D. U. Case, "Analysis of the cyber attack on the Ukrainian power grid," *Electr. Inf. Sharing Center*, vol. 388, no. 1, pp. 1–29, Mar. 2016.

[3] K. Proska, J. Wolfram, J. Wilson, D. Black, K. Lunden, D. K. Zafra, N. Brubaker, T. McLellan, and C. Sistrunk. (Nov. 2023). *Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology*. [Online]. Available: https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology

[4] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *Int. J. Electr. Power Energy Syst.*, vol. 99, pp. 45–56, Jul. 2018.

[5] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-physical power system (CPPS): A review on modeling, simulation, and analysis with cyber security applications," *IEEE Access*, vol. 8, pp. 151019–151064, 2020.

[6] S. Kim, K.-J. Park, and C. Lu, "A survey on network security for cyber–physical systems: From threats to resilient design," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 3, pp. 1534–1573, 3rd Quart., 2022.

[7] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1851–1877, 2nd Quart., 2019.

[8] V. K. Singh and M. Govindarasu, "Cyber kill chain-based hybrid intrusion detection system for smart grid," in *Wide Area Power Systems Stability, Protection, and Security*. Cham, Switzerland: Springer, 2021, pp. 571–599.

[9] B. Ahn, T. Kim, J. Choi, S.-W. Park, K. Park, and D. Won, "A cyber kill chain model for distributed energy resources (DER) aggregation systems," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Washington, DC, USA, Feb. 2021, pp. 1–5.

[10] A. Sreejith and K. S. Swarup, "MITRE ATT&CK for smart grid cyber-security," in *Cyber-Security for Smart Grid Control: Vulnerability Assessment, Attack Detection, and Mitigation*. Cham, Switzerland: Springer, 2024, pp. 59–73.

[11] N. K. Singh and V. Mahajan, "Analysis and evaluation of cyber-attack impact on critical power system infrastructure," *Smart Sci.*, vol. 9, no. 1, pp. 1–13, Jan. 2021.

[12] A. Ahmad, J. Webb, K. C. Desouza, and J. Boorman, "Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack," *Comput. Secur.*, vol. 86, pp. 402–418, Sep. 2019.

[13] B. Stojanović, K. Hofer-Schmitz, and U. Kleb, "APT datasets and attack modeling for automated detection methods: A review," *Comput. Secur.*, vol. 92, May 2020, Art. no. 101734.

[14] G. Laurenza, R. Lazzeretti, and L. Mazzotti, "Malware triage for early identification of advanced persistent threat activities," *Digit. Threats, Res. Pract.*, vol. 1, no. 3, pp. 1–17, Sep. 2020.

[15] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," in *Leading Issues in Information Warfare and Security Research*, vol. 1. Bethesda, MD, USA: Lockheed Martin, 2011.

[16] A. Hahn, R. K. Thomas, I. Lozano, and A. Cardenas, "A multi-layered and kill-chain based security analysis framework for cyber-physical systems," *Int. J. Crit. Infrastruct. Protection*, vol. 11, pp. 39–50, Dec. 2015.

[17] Mitre. *Industrial Control System (ICS) Techniques*. Accessed: Mar. 9, 2023. [Online]. Available: https://attack.mitre.org/techniques/ics/

[18] M. Assante and R. Lee. (Oct. 2015). *The Industrial Control System Cyber Kill Chain*. Accessed: Mar. 9, 2023. [Online]. Available: https://scadahacker.com/library/Documents/White_Papers/SANS%20-%20ICS%20Cyber%20Kill%20 Chain.pdf

[19] Mandiant Intell. Center. (Feb. 2013). *APT1: Exposing One of China's Cyber Espionage Units*. Accessed: Mar. 22, 2023. [Online]. Available: https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf

[20] E. Cole, *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization*. Amsterdam, The Netherlands: Elsevier, 2013.

[21] P. Chen, L. Desmet, and C. Huygens, "A study on advanced persistent threats," in *Proc. IFIP Int. Conf. Commun. Multimedia Secur.*, 2014, pp. 63–72.

[22] R. Kissel, "Glossary of key information security terms," NIST Interagency/Internal, Gaithersburg, MD, USA, Tech. Rep. 7298rev2, Jun. 2013.

[23] J. A. Lewis, "Computer espionage, titan rain and China," Center for Strategic Int. Studies-Technology Public Policy Program, CSIS, Washington, DC, USA, Tech. Rep., 2005, vol. 1.

[24] O. Thonnard, L. Bilge, G. O'Gorman, S. Kiernan, and M. Lee, "Industrial espionage and targeted attacks: Understanding the characteristics of an escalating threat," in *Research in Attacks, Intrusions, and Defenses*. Cham, Switzerland: Springer, Sep. 2012, pp. 64–85.

[25] C. Czosseck, R. Ottis, and A.-M. Talihärm, "Estonia after the 2007 cyber attacks," *Int. J. Cyber Warfare Terrorism*, vol. 1, no. 1, pp. 24–34, Jan. 2011.

[26] R. J. Deibert, R. Rohozinski, A. Manchanda, N. Villeneuve, and G. M. F. Walton, "Tracking GhostNet: Investigating a cyber espionage network," Inf. Warfare Monitor, Munk Centre Int. Stud., Univ. Toronto, Toronto, ON, Canada, Tech. Rep. 2, pp. 1–53, Mar. 2009.

[27] R. J. Deibert, and R. Rohozinski, "Shadows in the cloud: Investigating cyber espionage 2.0," Inf. Warfare Monitor, Munk Centre Int. Stud., Univ. Toronto, Toronto, ON, Canada, Tech. Rep. 3, pp. 1–58, 2010.

[28] B. Binde, R. McRee, and T. J. Connor, "Assessing outbound traffic to uncover advanced persistent threat," SANS Inst., Rockville, MD, USA, White Paper 1, pp. 1–35, 2011, pp. 1–35.

[29] McAfee. (Feb. 2011). *Global Energy Cyberattacks: 'Night Dragon*. Accessed: Mar. 23, 2023. [Online]. Available: https://www.mcafee.com/blogs/wp-content/uploads/2011/02McAfee_NightDragon_wp_draft_to_customersv1-1.pdf

[30] BBC News. (Oct. 30, 2013). *Adobe Hack Worse Than First Reported*. Accessed: Mar. 22, 2023. [Online]. Available: https://www.bbc.com/news/technology-24740873

[31] N. Perlroth. (Oct. 3, 2017). *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*. New York Times. Accessed: Mar. 22, 2023. [Online]. Available: https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html

[32] S. Haggard and J. R. Lindsay, "North Korea and the Sony hack: Exporting instability through cyberspace," East-West Center, JSTOR, New York, NY, USA, Tech. Rep. 117, pp. 1–8, May 2015.

[33] S. Gootman, "OPM hack: The most dangerous threat to the federal government today," *J. Appl. Secur. Res.*, vol. 11, no. 4, pp. 517–525, Sep. 2016.

[34] Y. B. Choi, "Organizational cyber data breach analysis of Facebook, Equifax, and Uber cases," *Int. J. Cyber Res. Educ.*, vol. 3, no. 1, pp. 58–64, Jan. 2021.

[35] S. Ghafur, S. Kristensen, K. Honeyford, G. Martin, A. Darzi, and P. Aylin, "A retrospective impact analysis of the WannaCry cyberattack on the NHS," *NPJ Digit. Med.*, vol. 2, no. 1, p. 98, Oct. 2019.

[36] S. Y. A. Fayi, "What Petya/NotPetya ransomware is and what its remidiations are," in *Proc. Adv. Intell. Syst. Comput.*, 2018, pp. 93–100.

[37] N. Daswani and M. Elbayadi, "The marriott breach," in *Big Breaches: Cybersecurity Lessons for Everyone*. Berkeley, CA, USA: Apress, 2021, pp. 55–74.

[38] E. Mikalauskas. (Jun. 7, 2021). *RockYou2021: Largest Password Compilation of All Time Leaked Online With 8.4 Billion Entries*. CyberNews. Accessed: Mar. 23, 2023. [Online]. Available: https://cybernews.com/security/rockyou2021-alltime-largest-password-compilation-leaked/

[39] J. Sadowski, "When data is capital: Datafication, accumulation, and extraction," *Big Data Soc.*, vol. 6, no. 1, pp. 1–12, Jan. 2019.

[40] W. A. Günther, M. H. R. Mehrizi, M. Huysman, and F. Feldberg, "Debating big data: A literature review on realizing value from big data," *J. Strategic Inf. Syst.*, vol. 26, no. 3, pp. 191–209, Sep. 2017.

[41] R. Baheti and H. Gill, "Cyber-physical systems," *Impact Control Technol.*, vol. 12, no. 1, pp. 161–166, Mar. 2012.

[42] Y. Liu, Y. Peng, B. Wang, S. Yao, and Z. Liu, "Review on cyber-physical systems," *IEEE/CAA J. Autom. Sinica*, vol. 4, no. 1, pp. 27–40, Jan. 2017.

[43] B. Miller and D. Rowe, "A survey SCADA of and critical infrastructure incidents," in *Proc. 1st Annu. Conf. Res. Inf. Technol.*, Calgary, AB, Canada, Oct. 2012, pp. 51–56.

[44] R. J. Turk. (Oct. 2005). *Cyber Incidents Involving Control Systems*. U.S.-CERT Control Syst. Secur. Center. Accessed: Mar. 23, 2023. [Online]. Available: https://www.osti.gov/biblio/911775

[45] R. Derbyshire, B. Green, D. Prince, A. Mauthe, and D. Hutchison, "An analysis of cyber security attack taxonomies," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW)*, London, U.K., Apr. 2018, pp. 153–161.

[46] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, Feb. 2011.

[47] R. M. Lee, M. J. Assante, and T. Conway, "ICS CP/PE (cyber-to-physical or process effects) case study paper—German steel mill cyber attack," ICS SANS, SANS, Rockville, MD, USA, Tech. Rep. pp. 1–15, Dec. 2014.

[48] A. Di Pinto, Y. Dragoni, and A. Carcano, "TRITON: The first ICS cyber attack on safety instrument systems. Understanding the malware, its communications and its OT payload," Proc. Black Hat, Las Vegas, NV, USA, Tech. Rep. 1, pp. 1–26, Aug. 2018.

[49] J. W. Goodell and S. Corbet, "Commodity market exposure to energy-firm distress: Evidence from the colonial pipeline ransomware attack," *Finance Res. Lett.*, vol. 51, Jan. 2023, Art. no. 103329.

[50] Microsoft Digit. Secur. Unit. (Apr. 27, 2022). *An Overview of Russia's Cyberattack Activity in Ukraine*. Accessed: Mar. 23, 2023. [Online]. Available: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

[51] M. Noguchi and H. Ueda, "An analysis of the actual status of recent cyberattacks on critical infrastructures," *NEC Tech. J.*, vol. 12, no. 2, pp. 19–24, Jan. 2018.

[52] D. Salmon, M. Zeller, A. Guzmán, V. Mynam, and M. Donolo, "Mitigating the Aurora vulnerability with existing technology," in *Proc. 36th Annu. Protection Relay Conf.*, Spokane, WA, USA, Oct. 2009, pp. 1–8.

[53] ENTSO-E. (Mar. 9, 2020). *ENTSO-E Has Recently Found Evidence of a Successful Cyber Intrusion Into Its Office Network*. Accessed: Mar. 23, 2023. [Online]. Available: https://www.entsoe.eu/news/2020/03/09/entso-e-has-recently-found-evidence-of-a-successful-cyber-intrusion-into-its-office-network/

[54] Inskit Group. (Feb. 28, 2021). *China-linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions*. Cyber Threat Anal. Accessed: Mar. 23, 2023. [Online]. Available: https://www.recordedfuture.com/redecho-targeting-indian-power-sector

[55] Black Lotus Labs. (Jun. 2021). *Suspected Pakistani Actor Compromises Indian Power Company With New ReverseRat*. Accessed: Mar. 23, 2023. [Online]. Available: https://blog.lumen.com/suspected-pakistani-actor-compromises-indian-power-company-with-new-reverserat/

[56] Eur. Space Policy Inst. (Oct. 2020). *The War in Ukraine From a Space Cyber Security Perspective*. Accessed: Mar. 23, 2023. [Online]. Available: https://www.espi.or.at/wp-content/uploads/2022/10/ESPI-Short-1-Final-Report.pdf

[57] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, "Analyzing the cyber-physical impact of cyber events on the power grid," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2444–2453, Sep. 2015.

[58] L. Che, X. Liu, T. Ding, and Z. Li, "Revealing impacts of cyber attacks on power grids vulnerability to cascading failures," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 66, no. 6, pp. 1058–1062, Jun. 2019.

[59] W. Sun, C.-C. Liu, and L. Zhang, "Optimal generator start-up strategy for bulk power system restoration," *IEEE Trans. Power Syst.*, vol. 26, no. 3, pp. 1357–1366, Aug. 2011.

[60] M. Glassman and M. J. Kang, "Intelligence in the Internet age: The emergence and evolution of open source intelligence (OSINT)," *Comput. Hum. Behav.*, vol. 28, no. 2, pp. 673–682, Mar. 2012.

[61] P. Larsen, S. Brunthaler, and M. Franz, "Automatic software diversity," *IEEE Secur. Privacy*, vol. 13, no. 2, pp. 30–37, Mar. 2015.

[62] E. Poremski and S. Liles, "Fusion of malware and weapons taxonomies for analysis," *J. Inf. Warfare*, vol. 14, no. 1, pp. 75–83, Jan. 2015.

[63] M. M. Yamin, M. Ullah, H. Ullah, and B. Katt, "Weaponized AI for cyber attacks," *J. Inf. Secur. Appl.*, vol. 57, Mar. 2021, Art. no. 102722.

[64] B. Guembe, A. Azeta, S. Misra, V. C. Osamor, L. Fernandez-Sanz, and V. Pospelova, "The emerging threat of AI-driven cyber attacks: A review," *Appl. Artif. Intell.*, vol. 36, no. 1, pp. 1–34, Dec. 2022.

[65] K. L. Chiew, K. S. C. Yong, and C. L. Tan, "A survey of phishing attacks: Their types, vectors and technical approaches," *Expert Syst. Appl.*, vol. 106, pp. 1–20, Sep. 2018.

[66] Exploit-DB. *Exploit Database*. Accessed: Mar. 9, 2023. [Online]. Available: https://www.exploit-db.com/

[67] Mitre. *Mitre Common Vulnerabilities and Exposures (CVE)*. Accessed: Mar. 9, 2023. [Online]. Available: https://cve.mitre.org/

[68] U. K. Singh, C. Joshi, and D. Kanellopoulos, "A framework for zero-day vulnerabilities detection and prioritization," *J. Inf. Secur. Appl.*, vol. 46, pp. 164–172, Jun. 2019.

[69] M. Kol and S. Oberman, "CVE-2020–11896 RCE and CVE-2020–11898 info leak," JSOF, Jerusalem, Israel, White Paper 1, pp. 1–27, Jun. 2020.

[70] L. Cheng, F. Liu, and D. Yao, "Enterprise data breach: Causes, challenges, prevention, and future directions," *Wiley Interdiscip. Rev. Data Mining Knowl. Discovery*, vol. 7, no. 5, pp. 1–14, Sep. 2017.

[71] P. Pourbeik, P. S. Kundur, and C. W. Taylor, "The anatomy of a power grid blackout—Root causes and dynamics of recent major blackouts," *IEEE Power Energy Mag.*, vol. 4, no. 5, pp. 22–29, Sep. 2006.

[72] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, R. Schulz, A. Stankovic, C. Taylor, and V. Vittal, "Causes of the 2003 major grid blackouts in north America and Europe, and recommended means to improve system dynamic performance," *IEEE Trans. Power Syst.*, vol. 20, no. 4, pp. 1922–1928, Nov. 2005.

[73] R. G. Little, "Controlling cascading failure: Understanding the vulnerabilities of interconnected infrastructures," *J. Urban Technol.*, vol. 9, no. 1, pp. 109–123, Apr. 2002.

[74] V. S. Rajkumar, A. Ştefanov, A. Presekal, P. Palensky, and J. L. R. Torres, "Cyber attacks on power grids: Causes and propagation of cascading failures," *IEEE Access*, vol. 11, pp. 103154–103176, 2023.

[75] Y. V. Makarov, V. I. Reshetov, A. Stroev, and I. Voropai, "Blackout prevention in the United States, Europe, and Russia," *Proc. IEEE*, vol. 93, no. 11, pp. 1942–1955, Nov. 2005.

[76] UCTE. (Aug. 2004). *Final Report of the Investigation Committee on the September 3 Blackout in Italy*. Accessed: Jul. 21, 2021. [Online]. Available: http://ns2.rae.gr/old/cases/C13/italy/UCTE_rept.pdf

[77] J. W. Bialek, "Why has it happened again? Comparison between the UCTE blackout in 2006 and the blackouts of 2003," in *Proc. IEEE Lausanne Power Tech*, Jul. 2007, pp. 51–56.

[78] J. J. Romero, "Blackouts illuminate India's power problems," *IEEE Spectr.*, vol. 49, no. 10, pp. 11–12, Oct. 2012.

[79] B. Schäfer and G. C. Yalcin, "Dynamical modeling of cascading failures in the Turkish power grid," *Chaos, Interdiscipl. J. Nonlinear Sci.*, vol. 29, no. 9, Sep. 2019, Art. no. 093134.

[80] S. Wilde. *9 August 2019 Power Outage Report*. Accessed: Dec. 7, 2022. [Online]. Available: https://www.ofgem.gov.uk/sites/default/files/docs/2020/01/9_august_2019_power_outage_report.pdf

[81] C. Makridis and B. Dean, "Measuring the economic effects of data breaches on firm outcomes: Challenges and opportunities," *J. Econ. Social Meas.*, vol. 43, nos. 1–2, pp. 59–83, Jul. 2018.

[82] CISA. *Critical Infrastructure in Energy Sector*. Accessed: Mar. 9, 2023. [Online]. Available: https://www.cisa.gov/energy-sector

[83] G. B. Anderson and M. L. Bell, "Lights out: Impact of the August 2003 power outage on mortality in New York, NY," *Epidemiology*, vol. 23, no. 2, pp. 189–193, Mar. 2012.

[84] V. R. Melnikov, V. V. Krzhizhanovskaya, A. V. Boukhanovsky, and P. M. A. Sloot, "Data-driven modeling of transportation systems and traffic data analysis during a major power outage in the Netherlands," *Proc. Comput. Sci.*, vol. 66, pp. 336–345, 2015.

[85] S. Küfeoğlu, "Economic impacts of electric power outages and evaluation of customer interruption costs," Doctoral thesis, Dept. Electrical Engineering Automation, Aalto Univ., Espoo, Finland, Mar. 9, 2023, pp. 1–64. [Online]. Available: https://aaltodoc.aalto.fi/handle/123456789/17867

[86] N. Kostyuk and Y. M. Zhukov, "Invisible digital front: Can cyber attacks shape battlefield events?" *J. Conflict Resolution*, vol. 63, no. 2, pp. 317–347, Feb. 2019.

[87] Y. Liu, R. Fan, and V. Terzija, "Power system restoration: A literature review from 2006 to 2016," *J. Modern Power Syst. Clean Energy*, vol. 4, no. 3, pp. 332–341, Jul. 2016.

[88] R. V. Yohanandhan, R. M. Elavarasan, R. Pugazhendhi, M. Premkumar, L. Mihet-Popa, and V. Terzija, "A holistic review on cyber-physical power system (CPPS) testbeds for secure and sustainable electric power grid—Part II: Classification, overview and assessment of CPPS testbeds," *Int. J. Elect. Power Energy Syst.*, vol. 137, May 2022, Art. no. 107721.

[89] R. L. S. de Oliveira, C. M. Schweitzer, A. A. Shinoda, and L. R. Prete, "Using mininet for emulation and prototyping software-defined networks," in *Proc. IEEE Colombian Conf. Commun. Comput. (COLCOM)*, Bogota, Colombia, Jun. 2014, pp. 1–6.

[90] V. S. Rajkumar, M. Tealane, A. Stefanov, A. Presekal, and P. Palensky, "Cyber attacks on power system automation and protection and impact analysis," in *Proc. IEEE PES Innov. Smart Grid Technol. Eur. (ISGT-Europe)*, Delft, The Netherlands, Oct. 2020, pp. 247–254.

[91] J. F. Hauer, N. B. Bhatt, K. Shah, and S. Kolluri, "Performance of 'WAMS East' in providing dynamic information for the north east blackout of August 14, 2003," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, Denver, CO, USA, Jun. 2003, pp. 1685–1690.

[92] A. Presekal, A. Stefanov, V. S. Rajkumar, and P. Palensky, "Attack graph model for cyber-physical power systems using hybrid deep learning," *IEEE Trans. Smart Grid*, vol. 14, no. 5, pp. 4007–4020, Sep. 2023.

[93] M. A. Khalaf and A. Steiti, "Artificial intelligence predictions in cyber security: Analysis and early detection of cyber attacks," *Babylonian J. Mach. Learn.*, vol. 2024, pp. 63–68, May 2024.

[94] A. Alsajri and A. Steiti, "Intrusion detection system based on machine learning algorithms: (SVM and genetic algorithm)," *Babylonian J. Mach. Learn.*, vol. 2024, pp. 15–29, Jan. 2023.

[95] R. H. K. Al-Rubaye and A. K. Türkben, "Using artificial intelligence to evaluating detection of cybersecurity threats in ad hoc networks," *Babylonian J. Netw.*, vol. 2024, pp. 45–56, Apr. 2024.

[96] S. S. Qasim and S. M. Nsaif, "Advancements in time series-based detection systems for distributed denial-of-service (DDoS) attacks: A comprehensive review," *Babylonian J. Netw.*, vol. 2024, pp. 9–17, Jan. 2024.

ALFAN PRESEKAL (Member, IEEE) received the bachelor's degree in computer engineering from Universitas Indonesia, in 2014, and the master's degree in secure software systems from the Department of Computing, Imperial College London, U.K., in 2016. He was an Assistant Professor of computer engineering with the Department of Electrical Engineering, Universitas Indonesia. He is currently a Researcher of cyber resilient power grids within intelligent electrical power grids with the Department of Electrical Sustainable Energy, Delft University of Technology. His research interests include cyber security, cyber-physical systems, and artificial intelligence.

ALEXANDRU ŞTEFANOV (Member, IEEE) received the M.Sc. degree from the University Politehnica of Bucharest, Romania, in 2011, and the Ph.D. degree from University College Dublin, Ireland, in 2015. He is currently an Associate Professor of intelligent electrical power grids with the Department of Electrical Sustainable Energy, TU Delft, The Netherlands. He is the Director of the Control Room of the Future (CRoF) Technology Centre. He is leading the Cyber Resilient Power Grids (CRPG) Research Group. His research interests include cyber security of power grids, resilience of cyber-physical systems, and next generation grid operation. He holds the professional title of Chartered Engineer from Engineers Ireland.

VETRIVEL SUBRAMANIAM RAJKUMAR (Graduate Student Member, IEEE) received the B.Eng. degree in electrical engineering from Anna University, India, in 2013, and the M.Sc. degree in electrical power engineering from Delft University of Technology, The Netherlands, in 2019. He is currently a Doctoral Researcher with the Intelligent Electrical Power Grids Group, Department of Electrical Sustainable Technology, Delft University of Technology. His research interests include cyber security and resilience for power grids.

IOANNIS SEMERTZIS (Graduate Student Member, IEEE) received the Diploma degree in electrical and computer engineering from the Democritus University of Thrace, Greece, in 2019, and the M.Sc. degree in electrical power engineering from Delft University of Technology, Delft, The Netherlands, in 2021, where he is currently pursuing the Ph.D. degree with the Department of Electrical Sustainable Energy. His research interests include cyber security, cyber-physical power systems, power system stability, and artificial intelligence for power system applications.

PETER PALENSKY (Senior Member, IEEE) received the M.Sc. degree in electrical engineering and the Ph.D. and Habilitation degrees from Vienna University of Technology, Austria, in 1997, 2001, and 2015, respectively. He co-founded an Envidatec, a German startup on energy management and analytics, and joined the Lawrence Berkeley National Laboratory, Berkeley, CA, USA, as a Researcher, and the University of Pretoria, South Africa, in 2008. In 2009, he appointed as the Head of the Business Unit on Sustainable Building Technologies, Austrian Institute of Technology (AIT), and later the first Principal Scientist of complex energy systems with AIT. In 2014, he was appointed as a Full Professor of intelligent electric power grids with TU Delft. He is active in international committees, such as ISO or CEN. His research interests include energy automation networks, smart grids, and modeling intelligent energy systems. He also serves as an IEEE IES AdCom Member-at-Large in various functions for IEEE. He is also the Editor-in-Chief of *IEEE Industrial Electronics Magazine* and an associate editor of several other IEEE publications and regularly organizes IEEE conferences.