IEEE Open Journal of the
Industrial Electronics Society

Received 1 December 2024; accepted 5 January 2025. Date of publication 8 January 2025;
date of current version 23 January 2025. The review of this article was arranged by Associate Editor G. Hancke.

Digital Object Identifier 10.1109/OJIES.2025.3527585

Enhancing Industrial Cybersecurity: Insights From Analyzing Threat Groups and Strategies in Operational Technology Environments

MUKUND BHOLE [1], THILO SAUTER [1,2] (Fellow, IEEE), AND WOLFGANG KASTNER [1] (Senior Member, IEEE)

[1]Institute of Computer Engineering, TU Wien, 1040 Vienna, Austria
[2]Center for Distributed Systems and Sensor Networks, University of Continuing Education Krems, 3500 Wiener Neustadt, Austria

CORRESPONDING AUTHOR: MUKUND BHOLE (e-mail: mukund.bhole@tuwien.ac.at)

This work was supported in part by the TÜV Austria's #SafeSecLab Research Lab for Safety and Security in Industry, in part by the Research Collaboration Between TU Wien and TÜV AUSTRIA, and in part by the TU Wien Bibliothek through its Open Access Funding Program.

ABSTRACT In recent years, concepts and components of information technology (IT) have made their way into the shop floor, today better known as operational technology (OT). The increasing interconnection and convergence of IT and OT have exposed industrial infrastructures to cyber attacks. In addition, they have become vulnerable to advanced persistent threats. This article examines real-world incidents, looking at the complex landscape of threat groups targeting OT environments and the tactic, technique, and procedures employed by these threat groups. Consequently, it highlights the need for increased vigilance in protecting OT environments, which can be done by using a variety of open-source threat intelligence platforms and databases, including Thai computer emergency response team (ThaiCERT), Malpedia by Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (Malpedia by FKIE), adversarial tactics, techniques, and common knowledge by massachusetts institute of technology research and engineering (MITRE ATT&CK), and Industrial Control Systems Cyber Emergency Response Team. We aim to provide relevant stakeholders (manufacturers, asset owners and system integrators), including Chief Information Security Officers, with information on emerging threat groups, attack victims and their locations, the origins of attacks, the tools and types of tools used, and the motivations behind these attacks. This understanding is crucial to improving defensive strategies based on relevant standards and frameworks and protecting OT environments against evolving cyber threats.

INDEX TERMS Operational technology (OT), security, threat group analysis.

I. INTRODUCTION

Operational technology (OT) environments encompass complex systems and technologies meticulously designed to supervise and regulate physical processes in diverse industrial sectors. Unlike its counterpart, information technology (IT), which centers around data manipulation and communication at an enterprise level, OT is dedicated explicitly to automating and monitoring industrial machinery, processes, and equipment. OT has emerged as the cornerstone of modern industrial advancement in the manufacturing, energy, oil and gas, industrial, petrochemical, and critical infrastructure domains.

In an era marked by the swift convergence of IT and OT, blending digital technologies with industrial infrastructure, the security of OT environments has emerged as a significant concern [1]. Security at the field level of the automation pyramid is not a completely new topic and has been discussed for more than two decades [2]. However, the rapid spread of IT concepts and components in the OT domain and the resulting tight interconnection resulting from this convergence have severely aggravated the problem. It has made OT increasingly vulnerable to threats that we used to know only from the IT world. Consequently, this has enabled and encouraged cyber adversaries to target and disrupt also OT systems. Among

these adversaries are also threat groups, such as *APT41* and *Dragonfly,* that now have the possibility to pivot and infiltrate a wide range of industrial infrastructure, exploiting the blurred boundaries between IT and OT security.

Threat groups benefit from substantial resources and excel in stealthy infiltrations of OT infrastructures, targeting sectors crucial for national interests by developing specialized malware for OT environments [3], [4]. Collaboration among threat groups in underground forums amplifies attacks on OT environments, facilitating synchronized efforts [5]. Threat groups are also leveraging artificial intelligence (AI) and machine learning (ML) techniques to increase the sophistication of the attack, posing an escalating threat to OT security [6], [7], [8]. Furthermore, they are interested in merging cyber capabilities with physical attacks on OT infrastructure, which sparks concerns about destructive cyber-physical assaults [9], [10].

Several notable incidents underscore the potentially catastrophic outcomes of cyber attacks on OT environments as follows.

1) The BlackEnergy malware was used in several high-profile attacks on OT environments by the Sandworm threat group, including the 2015 cyber attack on the Ukrainian power grid. BlackEnergy is a modular malware that can steal data, disrupt operations, and cause physical damage [11].
2) Industroyer malware was used in a cyber attack by the Dragonfly threat group on a Ukrainian electricity distribution company in 2016. Industroyer is sophisticated malware that can target both IT and OT systems, causing physical damage by disrupting the operation of critical infrastructures [12].
3) The VPNFilter malware was discovered in 2018 and targets Virtual Private Network (VPN) devices that connect OT networks to the Internet used by the threat group Sofacy (APT28). VPNFilter can steal data, disrupt operations, and deny access to critical systems [13].
4) The Triton malware was discovered in 2020 and is sophisticated malware used by the threat group TEMP.Veles targeting Industrial Control Systems (ICS), capable of causing physical damage by disrupting the essential operation of infrastructure [14].
5) The EKANS ransomware, discovered in December 2019 and more prevalent in early 2020, is used by the Turla threat group and targets explicitly ICS and OT networks. It encrypts files crucial to industrial processes, such as files used in Supervisory Control and Data Acquisition (SCADA) systems, Human Machine Interfaces (HMIs), and Programmable Logic Controllers (PLCs), demanding ransom payments for decryption keys [15].
6) The Colonial Pipeline ransomware attack, discovered in May 2021, targeted the major fuel pipeline operator in the US by the threat group Carbanak (Anunak). Using DarkSide ransomware, it encrypted crucial OT systems responsible for managing pipeline operations [16].
7) The Pipedream malware was discovered in early 2022 and reported by Dragos to have been created by the Chernovite threat group. Although there have been no reported attacks using Pipedream, it explicitly targets ICS and OT components, including PLCs, SCADA systems, and the Codesys software platform used to program PLCs. Pipedream is capable of disrupting or manipulating industrial processes, stealing data, and causing physical damage [17].

A common denominator in all such attacks is that it starts with infiltration of IT systems before proceeding to the actual OT level. Defenders must, therefore, implement robust cybersecurity measures to mitigate these evolving threats. The particular challenge is that many OT environments heavily rely on legacy systems, often with unpatched vulnerabilities, which facilitates attacks [9]. Before creating a defense strategy, stakeholders should carefully study the tactic, technique, and procedure (TTP) used by the threat actors. This *modus operandi* of threat groups has been well studied in the IT domain [18], [19], [20], [21]. However, little attention has been given so far to specific OT aspects.

This article aims to analyze comprehensively the complex landscape of advanced persistent threats (APTs) that have OT environments as their ultimate target. It explores different risk and vulnerability aspects while examining the Tactic, Technique, and Procedures (TTPs) used by the adversaries. The rest of this article is organized as follows. Section II provides related work on threat groups or APTs, Section III offers a comprehensive analysis of threat groups in OT environments, Section IV provides the results on the analysis of threat groups in OT environment, Section V presents the phases of the ICS cyber-kill chain procedure followed by threat groups and their impact on OT environments, while Section VI discusses the interpretation of statistical analysis of threat groups. Section VII provides strategies for defending against threat groups and malware. Finally, Section VIII concludes this article.

II. RELATED WORK

APT or threat group attribution is a complex challenge requiring a holistic approach, combining definitions, characteristics, and attack execution across both IT and OT environments.

Hussain et al. [22] overview APTs and their communication mechanisms, detailing how compromised hosts interact with command and control (C2) servers for command issuance and data exfiltration via persistent malware. However, the study focuses on IT environment detection frameworks and omits OT environment attack methodologies and preventive measures. Talib et al. [23] studied potential solutions for detecting APT beaconing, emphasizing communication channel-based techniques to detect C2 malware and beaconing activities.However, defense requires a layered approach beyond identifying communication channels; the study does not identify specific sectors targeted by APTs or the layers of architecture affected. Alshamrani et al. [21] examined the APT lifecycle, scrutinizing existing detection tools for

identifying different stages of APT attacks and exploring machine learning approaches to enhance threat detection systems. While the objective of their study aligns with ours, it neither address sector-specific issues in OT environments nor provide data-backed argumentation. Lemay et al. [18] surveyed open-source literature on APT actors and their activities up to 2017, emphasizing APT operations over defense or detection approaches. While this aligns with our goal of identifying research gaps in APTs, it neither cover sector-specific nor OT-specific threat groups.

Kotenko et al. [24], Huang et al. [25], and Muhammed and Das [26] examined cybercrime services and tools from a value chain perspective, identifying 24 key activities and their interrelations. While their analysis highlights the specialization and collaboration in cyber attacks, it neither addresses country-specific nor sector-specific attacks in OT environments. Bahrami et al. [19] provided a comprehensive overview of TTPs for APT, analyzing 22 APT groups and their 40 attacks. Their study outlined seven phases of the cyber kill chain: reconnaissance, weaponization, delivery, exploitation, installation, C2, and action on objectives (AOO). However, their overview lacks OT-specific and sector-specific attacks, whereas our study analyses 120 threat groups across the ICS/OT sector. Singh et al. [20] examine APT modeling and behavioral patterns, including various APT types and zero-day exploits. Their research focuses on clustering, learning, and extraction techniques. Models, such as the Kill Chain [27], Attack Tree [21], Attack Pyramid [28], Attack Graph [29], Markov model [30], Network Evolution [31], Diamond Model [32], Q Model [33], and Enterprise Commercial Model [34], outline APT attack attribution. Although aligned with our goals, the study still lacks coverage of sector-specific ICS/OT attacks.

Sundaram et al. [35] proposed an active defense mechanism for OT that involves introducing noise into the OT network to detect unauthorized manipulations by APTs and insider threats. However, their study does not address how TTPs might evolve in response to the implemented defense mechanisms. Krasznay and Gyebnár [36] developed a framework for sharing information on the TTPs of threat actors targeting the OT/ICS environment in the energy sector, utilizing a honeypot. While their study provides valuable insights into threat intelligence, it lacks detailed information on specific TTPs and is limited to a single sector. Jadidi and Lu [37] proposed a three-phase threat hunting framework for ICS/OT networks that integrates the Diamond Model [32] and adversarial tactics, techniques, and common knowledge by massachusetts institute of technology research and engineering (MITRE ATT&CK). This framework aims to identify TTPs and visualize attack routes toward targets. However, it does not offer a comprehensive overview of the TTPs and APTs across the broader OT/ICS environment

The novelty of our work, compared to the studies mentioned, lies in its focus on the OT environment. This area still has significant research gaps, particularly regarding the current landscape of APT/ threat groups exploiting OT systems. By investigating data-backed arguments on sector-specific analyses, emerging threat groups in OT environments, their TTPs, and identifying the countries responsible for or affected by these attacks, we aim to provide new directions for future research.

III. ANALYSIS OF THREAT GROUPS

There are several open-source threat intelligence platforms and databases that provide information about known threat groups, their activities, tactics, and techniques. The challenge is that they are not using uniform data formats and have different coverage of incidents, which makes harmonizing information difficult. In our survey, we try to collate information from several sources in a systematic way.

A. DATA SOURCES

Cybersecurity professionals often use a combination of open-source intelligence, commercial threat intelligence feeds, and proprietary research to develop a comprehensive understanding of threat groups and their activities. Security researchers frequently study TTPs to create "threat profiles" that assist in identifying the origin, intent, and capabilities of a threat group. This information is crucial for comprehending the threat landscape, devising effective defenses, and responding to incidents. Notable sources, include Threat Group Cards by Thai computer emergency response team (ThaiCERT) [38], Malpedia by Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) [39], MITRE ATT&CK [40], and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) [41]. They are excellent resources for analyzing cyber threats targeting industrial systems, and these data sources also periodically include reports published by various OT security service providers, for instance, Dragos, Darktrace, FireEye, Nozomi Networks, Claroty, Forescout, and Kaspersky.

Specifically, ThaiCERT provides valuable insights into threat groups focused on sectors like energy and manufacturing, highlighting their tools and motivations. MITRE ATT&CK offers a structured framework for mapping attacks to the ISA-95 model, detailing the TTPs used by threat actors. Malpedia specializes in identifying malware families and tools associated with these groups, while ICS-CERT delivers incident reports specifically related to ICS environments, identifying affected infrastructure, industries, and the motivations behind the attacks. Together, these sources provide a comprehensive view of threats to critical infrastructure.

In contrast, platforms like EuRepoC[1] primarily focus on strategic-level intelligence and broad cybercrime trends rather than providing detailed, tactical data on specific threats or incidents. This limits their suitability for the purpose of this article. Although the platform updates data daily, a notable drawback is the inconsistent data quality, with many parameters frequently marked as "information not available." In addition, substantial manual effort is required to extract

[1] [Online]. Available: https://eurepoc.eu/

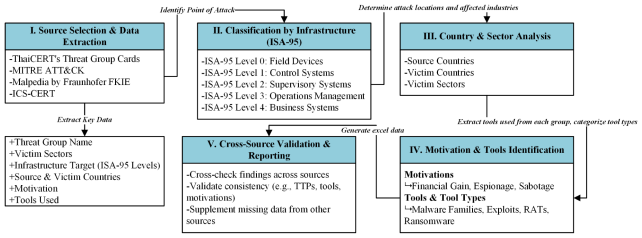

FIGURE 1. Methodology for the analysis of the threat groups.

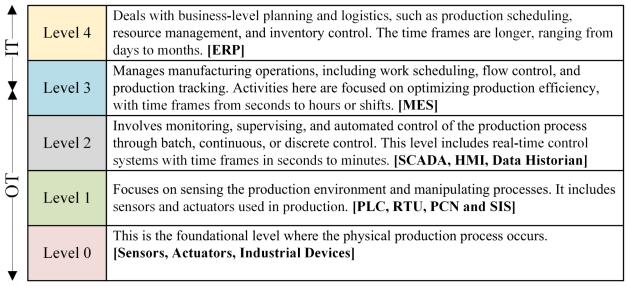

FIGURE 2. Levels in industrial automation based on the ISA-95 standard with associated functionalities [43].

the industry-specific insights necessary for analyzing threats to ICS and critical infrastructure. By comparison, resources, such as ThaiCERT and MITRE ATT&CK, offer more granular, timely, and technical information on TTPs, tools, and targeted sectors, making them more relevant for understanding specific threats to industrial environments.

B. METHODOLOGY

In order to collate information from the diverse data sources, we follow a multiphase methodology shown in Fig. 1. The methodology begins with *source selection and data extraction*, where threat group information is gathered from sources, such as ThaiCERT's Threat Group Cards, MITRE ATT&CK, Malpedia by Fraunhofer FKIE, and ICS-CERT. Key data points—including threat group names, targeted sectors, infrastructure levels [based on ISA-95 (see Fig. 2)], countries involved, motivations, and tools—are extracted.

In the *Classification by Infrastructure* phase, attacks are mapped to ISA-95 levels, ranging from Level 0 (field devices) to Level 4 (business systems), pinpointing the level of targeted infrastructure. Next, in the *Country and Sector Analysis* phase, source and victim countries and targeted sectors are identified. Moving to *Motivation and Tools Identification*, motivations, such as financial gain, espionage, or sabotage, are determined, along with categorizing the tools each threat group uses. Finally, the *Cross-Source Validation and Reporting* phase ensures consistency and fills gaps by cross-referencing findings across sources.

As the structures of the used databases vary, the application of the methodology varies in details, too. For ThaiCERT's Threat Group Cards, it focuses on victim sectors within critical industries, such as energy, manufacturing, and petrochemicals. In the *Classification by Infrastructure* phase, the analysis emphasizes attacks on ISA-95 Levels 0 to 3. Victim countries are identified during *Country and Sector Analysis*, and motivations and tools used by attackers are analyzed in *Motivation and Tools Identification.*

In MITRE ATT&CK, process starts by identifying relevant TTPs, particularly those affecting ISA-95 Levels 0 to 3, and mapping them to specific infrastructure levels. Threat groups using these TTPs, along with tools and motivations, are analyzed, with a focus on state-sponsored activities documented in MITRE ATT&CK.

In Malpedia by Fraunhofer FKIE, after data extraction on threat groups, we analyze corresponding malware families, tools, and affected countries. Malpedia may lack direct motivation or ISA-95 information, so these are inferred in the *Motivation and Tools Identification* phase when possible.

ICS-CERT advisories provide detailed insights into targeted infrastructure, especially in ICS incidents. These advisories facilitate detailed classification by ISA-95 level and allow for a deeper look into affected industries and regions during *Country and Sector Analysis*. Attack motivations—financial, espionage, or sabotage—are assessed in *Motivation and Tools Identification*, along with specific malware or exploits associated with industrial systems.

Using this methodology, we compiled information on approximately 443 threat groups, with 120 of them targeting OT/ICS environments in industrial sectors, such as manufacturing, energy, oil and gas, industrial, petrochemical, and critical infrastructure. The collated data from the methodology have been made publicly available in the dataset [42]. The platforms and databases used in the analysis may not cover all threat groups, but they do offer valuable insights into the latest threats and trends in the OT cybersecurity landscape.

IV. RESULTS OF THE ANALYSIS

A. THREAT ACTOR GROUP

Numerous threat actors pose significant risks to industries in the realm of OT. These threat actors encompass diverse entities, each with distinct motivations and capabilities. Fig. 3(a) presents the statistical analysis of threat groups that conducted attacks up until June 2023. The data reveals that the *Lazarus Group (also known as Hidden Cobra, Labyrinth Chollima)* accounted for the highest percentage of approximately 10% of overall attacks, followed closely by the *Lockbit Gang and Sofacy (also known as APT 28, Fancy Bear, Sednit)*, both contributing to approximately 8.5% of attacks on OT environments and so forth.

B. VICTIM SECTOR

Attacks on OT environments in different sectors can result in significant operational disruptions. Manufacturing production lines may come to a halt, causing delays in product delivery. Energy, oil, and gas facilities might experience shutdowns or disruptions in the supply chain, leading to energy shortages

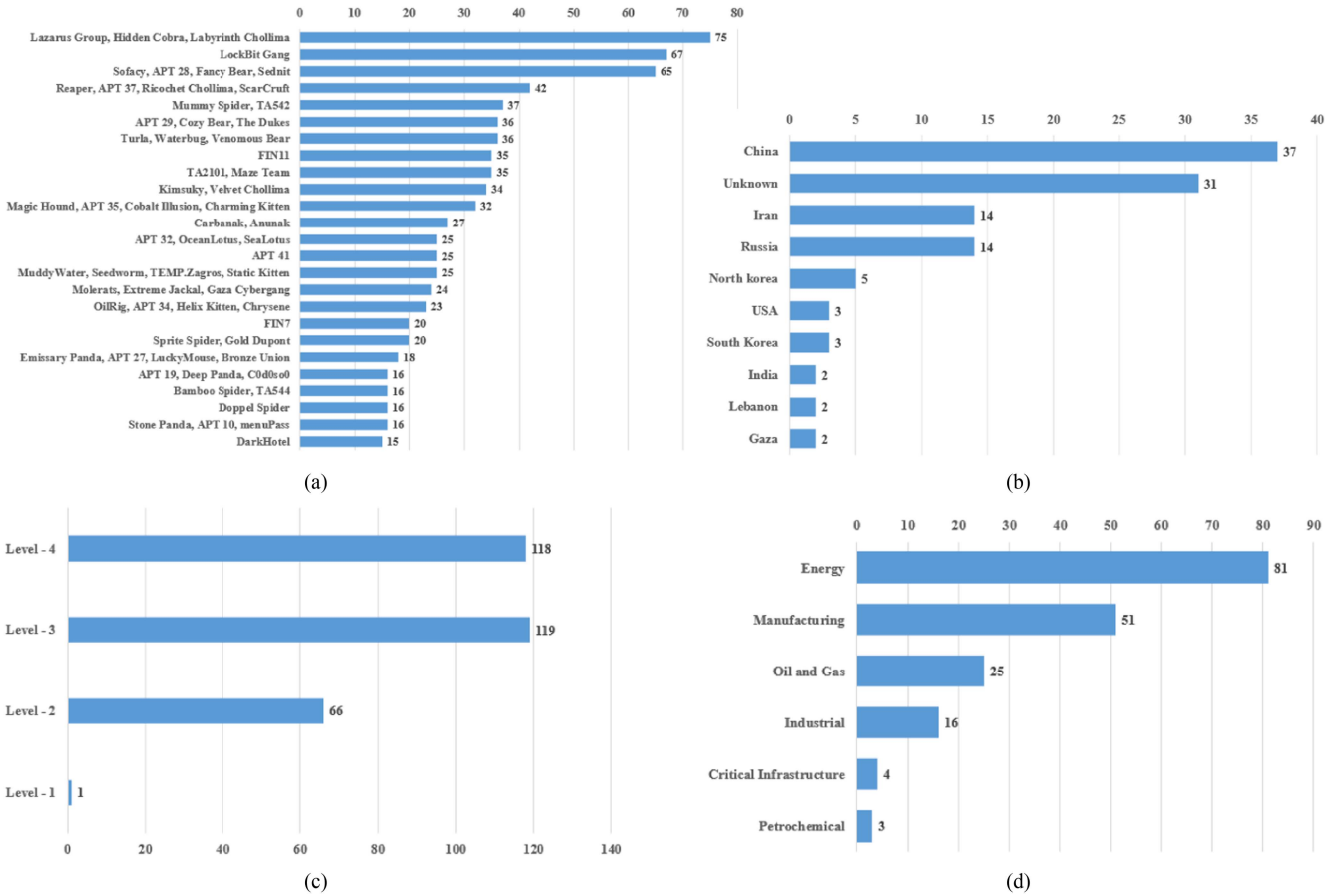

FIGURE 3. (a) Top 25 Threat Groups (with alias), (b) Top 10 Threat Source Countries, (c) ISA-95 Level-Based Attacks by Threat Groups, (d) Threat Groups Victim Sector based on [42].

and price fluctuations. Petrochemical plants could suffer from equipment malfunctions, affecting their output. A high-profile attack on an OT environment can tarnish the reputation of the impacted organization or industry. Customers, partners, and investors might lose trust in the organization's capacity to safeguard critical infrastructure, potentially losing business and brand value. Fig. 3(d) presents a statistical analysis of the affected victim sectors, along with the number of threat groups targeting each respective sector. The *energy sector* emerges as the most frequently attacked, contributed by 67.5% of the threat groups, followed by *manufacturing* with 42.5%, and *oil and gas* with 20.8%.

C. OT INFRASTRUCTURE TARGET LEVEL

In industrial automation, the convergence of two domains within ICS, namely, IT and OT, has emerged as the driving force behind Industry 4.0. Adopting cutting-edge software technologies, business intelligence, and analytics propels this evolution. Referring to the ISA-95 automation pyramid [43] (see Fig. 2 for a depiction of the related activities at each level), IT is positioned at Level 4 according to the standard. It governs business planning and logistics, encompassing data distribution software, data centers, corporate networks, and enterprise systems for data processing. Furthermore, OT occupies a position from Level 0, extending up through Level 2, and at times even encompassing Level 3. Its purview encompasses oversight of manufacturing operations and controls, including data acquisition systems, process plants, field equipment, human interfaces, and control networks. Fig. 3(c) illustrates a statistical analysis of the most targeted levels based on ISA-95. It reveals that *Level 3* is the most frequently attacked, targeted by 99% of threat groups, followed by *Level 4* with 98%, *Level 2* with 55%, and *Level 1* with approximately 1%.

D. SOURCE COUNTRY OF THREAT GROUP

Attributing cyber threat groups to specific source countries can present challenges and complexities due to using various techniques, such as proxy servers, VPNs, and false flag operations. These techniques allow attackers to conceal their actual locations and identities. Moreover, certain threat actors intentionally obfuscate their origins to avoid detection and attribution.

However, cybersecurity researchers and experts often analyze diverse indicators and TTPs employed in cyber attacks to formulate informed assessments about the likely origin

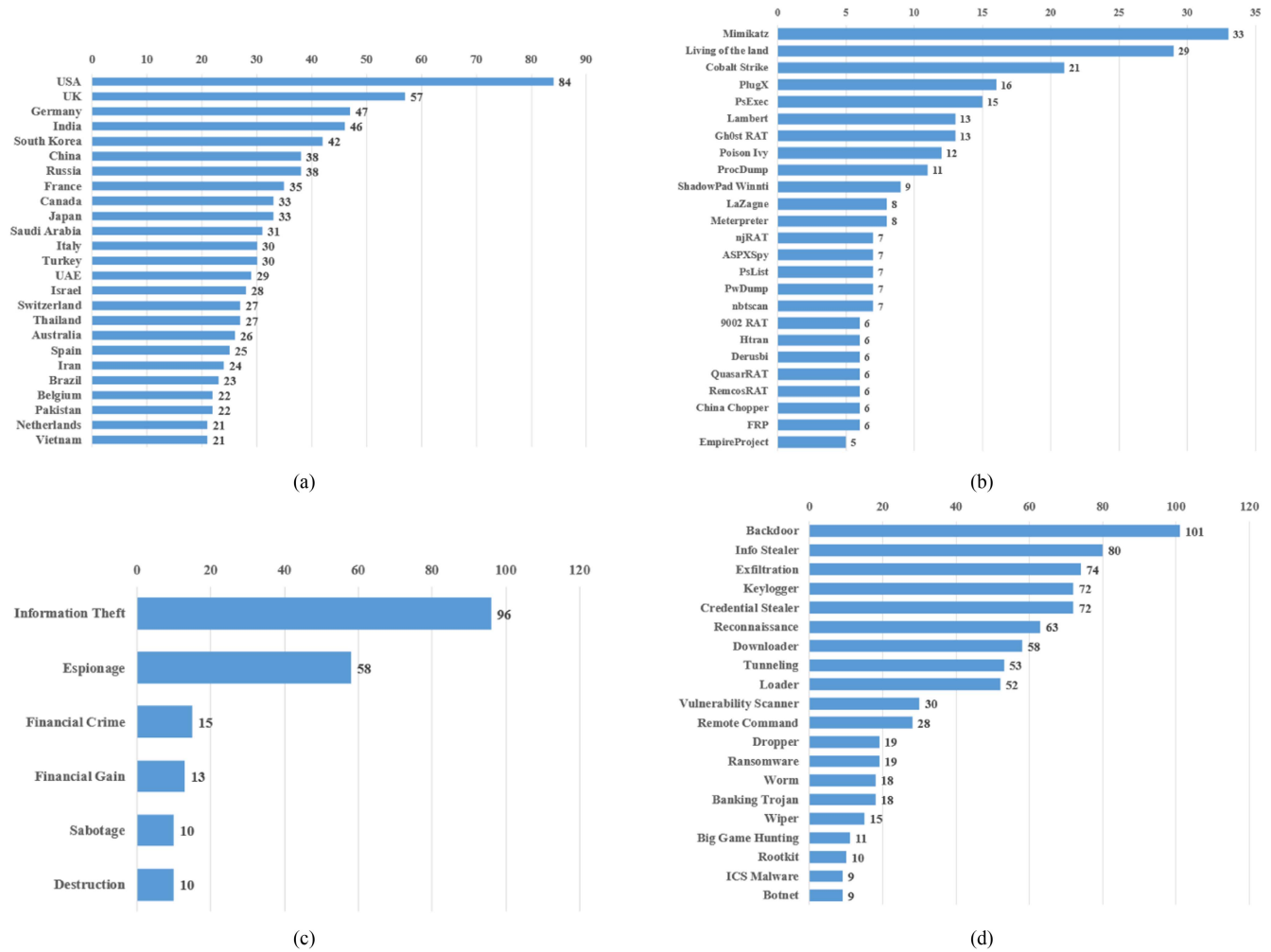

FIGURE 4. **(a) Top 25 victim countries. (b) Top 25 tools used by threat group. (c) Threat group attack motivation. (d) Top 20 type of tool used based on [42].**

of threat groups. Despite these challenges, continuous research and collaboration within the cybersecurity community enhance the accuracy of attribution and deepen the comprehension of the global threat landscape.

Fig. 3(b) displays a statistical analysis of the threat landscape, indicating the countries of origin for the threat groups. *China* emerges as the primary source, accounting for 30.8% of the threat groups, followed by *unidentified countries* at 25.8%, *Iran* and *Russia* at 11.6%, and others.

E. VICTIM COUNTRY OF ATTACK

The specific attribution of attacks to victim countries can be intricate and subject to change over time; certain countries are known to be more frequently targeted. Recognizing that these attacks can impact multiple countries is essential, and the roster may shift as new threats and campaigns emerge. Cyber attacks have the potential to affect numerous countries and organizations worldwide. While it is possible to report and analyze specific incidents and attacks, it is crucial to avoid making generalizations by assuming that threat groups exclusively focus on particular countries. Cyber-attacks represent a global phenomenon; victims can be identified in diverse countries and industries.

Fig. 4(a) illustrates a statistical analysis of countries frequently targeted due to their essential industrial infrastructure, which is critical for the operation of their economies. For instance, the *United States* has emerged as the primary target, being targeted by 70% of threat groups, hosting numerous major manufacturing plants, oil and gas pipelines, and power plants. These facilities are potential targets for threat groups aiming to disrupt or harm critical infrastructure. Following the *United States* are the *United Kingdom* at 47.5%, *Germany* at 39%, and other countries.

F. MOTIVATION OF ATTACK

As mentioned in the Section I, the motivation of threat groups varies depending on the specific goals they aim to achieve. Based on the analyzed data, we have observed that among the *120* threat groups, the outcomes of their motivations are illustrated in Fig. 4(c). Approximately 80% of the threat groups are motivated by *information theft*, while approximately 48% of them focus on *espionage*, and so forth.

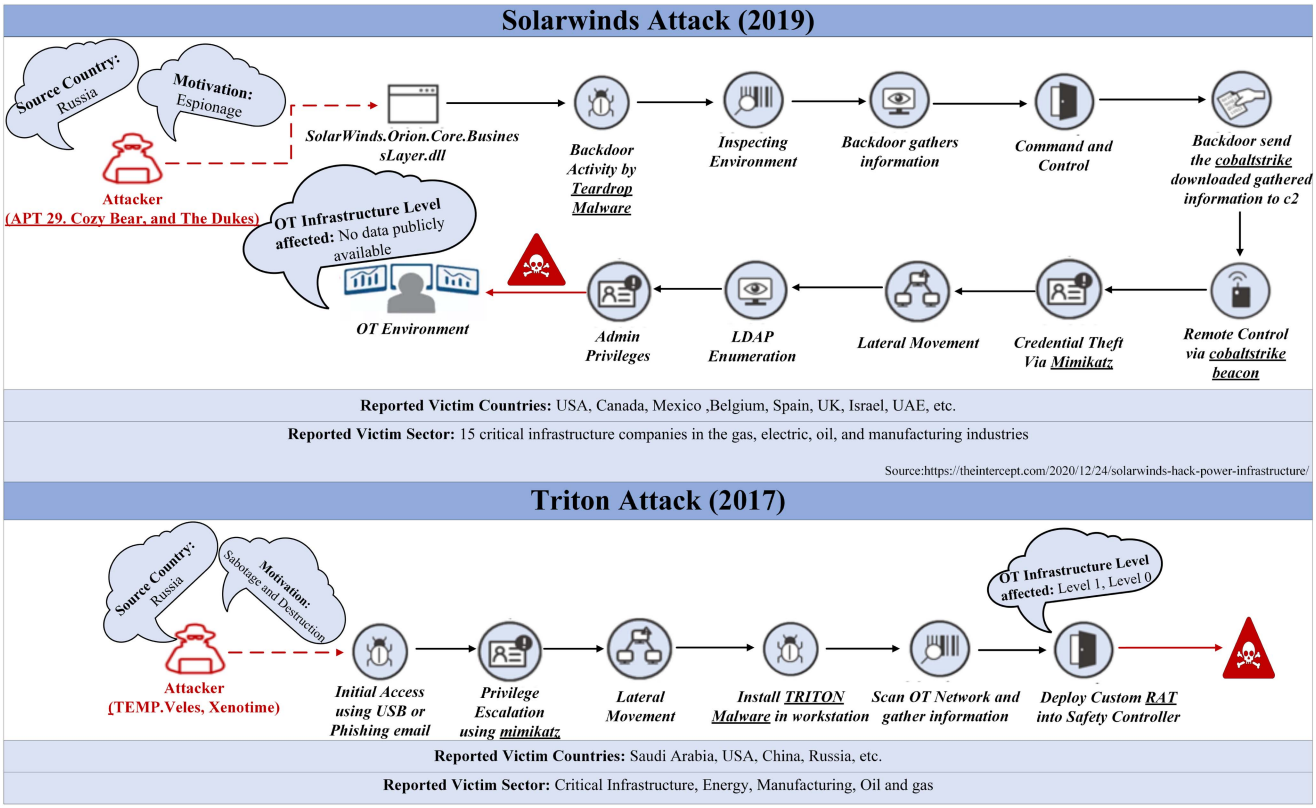

FIGURE 5. ICS cyber-kill chain procedure phases and impact of Solarwinds and TRITON attack on OT environment.

G. TOOLS USED IN ATTACK

Considerable research has been undertaken to study the selection of tools utilized by threat groups when targeting specific entities. Threat actors often follow discernible patterns in their attacks on these entities, and devising a strategy to counteract these tools could prove highly effective. The functionalities of all the tools are detailed in Table 1. Fig. 4(b) illustrates the various tools employed by the analyzed threat groups, with the *Mimikatz* tool being used by these threat groups approximately 28% of the time, followed by *Living off the Land* tools at 24.1%, *Cobalt Strike* at 17.5%, and others.

H. TYPE OF TOOLS USED IN ATTACK

The different types of malware cover a variety of malicious software; most malware is designed to exploit systems for the benefit of cybercriminals. Understanding the various types of malware is crucial in protecting devices and systems from cyber-attacks. Comprehending the different types of tools is essential in safeguarding from potential compromises. Fig. 4(d) displays the percentage usage of tool types by the threat groups, with *Backdoors* being used the most, accounting for 84% of the time, followed by *Info Stealers* at 66%, *Exfiltration tools* at 61%, and others.

V. ICS CYBER-KILL CHAIN PROCEDURE

We use the SANS ICS cyber kill chain [44], [45], a framework for dissecting complex attacks into nonexclusive stages. This two-stage model outlines an attacker's steps to target and compromise an ICS. Understanding these stages allows defenders to implement security measures to disrupt the attack process and mitigate risks. The stages of the ICS cyber kill chain are:

Stage 1: Reconnaissance—The attacker gathers information about the target ICS/OT environment, such as scanning for vulnerabilities, identifying devices and systems, and understanding the overall architecture.

Stage 2: Weaponization—The attacker uses the gathered information to develop and test tools or exploits to attack the ICS/OT. This may involve creating custom malware or modifying existing tools to target specific ICS vulnerabilities.

Fig. 5 illustrates the ICS cyber-kill chain procedure along with the attack source country, attack motivation, reported victim countries, and reported victim sectors, OT infrastructure level affected in relation to the threat group analysis (cf., Section III) for two distinct attacks: the SolarWinds and TRITON attacks.

The SolarWinds attack [46], attributed to the Russian APT group Cozy Bear (APT29), was a supply chain breach that infiltrated both SolarWinds' servers and customer networks. During the reconnaissance phase, attackers likely gathered information from public sources, industry reports, or even social media to plan how to exploit SolarWinds' software as an initial access vector. SolarWinds' software, designed for network monitoring, extends to OT levels, including SNMP networks and devices used in industrial and building

TABLE 1. Functionalities of Tools Used by Threat Groups

Tool	Functionality
Mimikatz	Credential theft tool, primarily used for extracting plaintext passwords, hashes, and tickets from memory.
Living off the Land	Refers to the use of legitimate system tools and functionalities by attackers for malicious purposes, making detection more challenging.
Cobalt Strike	Framework for adversary simulation and red team operations, facilitating post-exploitation activities, command and control, and lateral movement.
PlugX	RAT is designed for targeted attacks, allowing attackers to control compromised systems.
PsExec	Microsoft Sysinternals tool used for executing processes on remote systems, often employed for lateral movement in network exploitation.
Lambert	Part of the Equation Group's toolset, associated with sophisticated cyber espionage activities.
Gh0st RAT	RAT used for unauthorized access and control of compromised systems.
Poison Ivy	RAT with features for surveillance, data theft, and control of infected systems.
ProcDump	Sysinternals tool for creating process dumps is often used for analyzing and troubleshooting software.
ShadowPad Winnti	Backdoor is associated with the Winnti Group, known for targeted attacks against the gaming industry and other sectors.
LaZagne	Credential recovery tool, similar to Mimikatz, focuses on retrieving passwords from various applications.
Meterpreter	A payload within the Metasploit framework, providing a wide range of post-exploitation capabilities on compromised systems.
njRAT	RAT is used for remote control, surveillance, and data theft.
ASPXSpy	Webshell (a tool enabling a web server to be remotely accessed) is used for unauthorized access and control of web servers.
PsList	Sysinternals tool for listing detailed information about processes.
PwDump	Tool for extracting password hashes from Windows systems.
nbtscan	Network tool for discovering and enumerating NetBIOS shares.
9002 RAT	RAT known for evading detection and maintaining persistence on compromised systems.
Htran	Covert communication tool for creating hidden communication channels.
Derusbi	Backdoor are associated with various cyber threat groups, including APT17.
QuasarRAT	RAT with features for keylogging, screenshot capture, and more.
RemcosRAT	RAT with capabilities for remote control and surveillance.
China Chopper	Webshell often used by Chinese threat actors for unauthorized access to web servers.
FRP	Network tunneling tool for bypassing firewalls and accessing restricted networks.
EmpireProject	Post-exploitation framework for offensive security operations, similar to Cobalt Strike.

automation. In the weaponization phase, the Teardrop malware was injected into SolarWinds' update servers to exploit vulnerabilities in SolarWinds Orion and provide remote access. The attack implanted a malicious payload within SolarWinds' Orion platform software, specifically in *SolarWinds.Orion.Core.BusinessLayer.dll*. Subsequently, teardrop malware was deployed, creating a backdoor for collecting network information and establishing connections with a C2 server. Through Cobalt Strike, the attacker gained remote access, facilitating credential theft and privilege escalation. Mimikatz was employed for credential theft, enabling lateral movement within the network, LDAP enumeration, and obtaining admin privileges. With admin access, the attacker could have compromised the OT environment with ease.

According to the Schneider Electric analysis and disclosure [47], the Triton attack was executed through a phishing campaign and attributed to the Russian APT group TEMP.Veles (also known as Xenotime). In the Triton attack [48], it appears that the attackers attempted to implant a remote access trojan (RAT) within the Triconex safety instrumented system (SIS). During the reconnaissance phase, the attackers likely gathered information from industry publications, ICS vendor documentation, or even by exploiting zero-day vulnerabilities. They studied ICS protocols, identified vulnerabilities in Triconex SIS, and developed customized malware later named Triton (or Trisis). In the weaponization phase, initial access was possibly gained through phishing emails, insecure remote access, or USB infiltration. After gaining access, the attackers moved laterally within the compromised system and achieved privilege escalation using Mimikatz. Once inside the workstations, the attackers installed the Triton malware. Triton then scanned the OT network to gather information on PLCs and safety controllers, subsequently deploying a custom RAT to reprogram them. This action led to a safety incident, resulting in production downtime. Both Triton and SolarWinds attacks exemplify how successful ICS attacks often initiate within a victim's IT systems and extend into OT environments. In the Triton incident, attackers first compromised the IT network before moving into the OT system. In contrast, the SolarWinds attack exploited a supply chain vulnerability that allowed attackers to infiltrate IT networks, which, in some cases, provided access to OT systems as well.

VI. DISCUSSION

In security management teams, by increasing situational awareness in OT environments, threat analysis enables organizations to understand new risks and ways in which these risks can be managed. This analysis allows us to see specific multidimensional insights across different parameters.

Examining *victim sectors* makes it possible to develop more customized protection capable of dealing with problems and risk needs in each sector. Despite every industry's unique features, some recurrent patterns of threats and vectors

of attacks are dissimilar. Recognizing common weaknesses and strategies can offer the opportunity to build interindustry threat knowledge and defensive strategy. This analysis helps organizations meet regulatory controls specific to a sector or industry. As Fig. 3(d) shows, the number of attacks on sectors, such as energy, manufacturing, oil, and gas, shows that these sectors primarily depend on OT systems.

The principle of the *target level* helps determine the scale of the potential damage that may arise from cyber-attacks on some components of the OT infrastructure. This evaluation can help risk management teams and organizations use their resources effectively and strategically to implement ways of mitigating the most vulnerable targets as depicted in Fig. 3(c); once the target level is reached, it is understood that the majority of attack attempts are directed at the superordinate control levels, often IT systems, i.e., ISA-95 levels 3 and 4, which are of utmost importance. Such levels, for instance, usually consist of core production information, e.g., the schedules, the specifications, and quality control data. Attacks on those layers often expose threat actors to proprietary information and intellectual property, putting the company's competitiveness and continuity at risk.

The *source country* can help measure the potential aims of each attack. In cases where the source country is known, it becomes possible for the organizations to utilize diplomatic means in reporting the cyber incidences and to seek assistance concerning investigations, mitigation actions, sanctions, and counteractions. On the contrary, Fig. 3(b) shows countries that might have high OT exploitation capabilities, such as China, Iran, and Russia.

By assessing the *victim country*, we can estimate the degree to which the nation's OT systems may be impacted by hostile actions. This assessment provides the basis for determining the level of the threat bearing on national and public security and safety. In addition, examining the victim country enables an understanding of the cyber threats in more geographical contexts, which allows organizations to stay updated about foreign cyberspace incidents and modify their protective measures. As seen in Fig. 4(a), it interprets the higher adoption of OT in countries, such as the USA, U.K., Germany, and many more. Some countries might have even higher adoption of OT environments. However, they do not face any attacks. The reasons might be that they do not prefer to report those incidents, they have resilient security measures, or attackers do not have any motivation to attack.

The motivation behind an attack could help prioritize the order, in which the vulnerabilities must be patched or procedures to contain them. Such vulnerabilities are more likely to be exploited and thus warrant urgent attention for mitigation. As illustrated in Fig. 4(c), attacks that are motivated by information and economic purposes of espionage can have adverse effects on supply chains in OT environments, national security, critical infrastructure, and the economy. Those with a higher impact could require high levels of resource allocation for defensive efforts and for providing fast incident response capabilities.

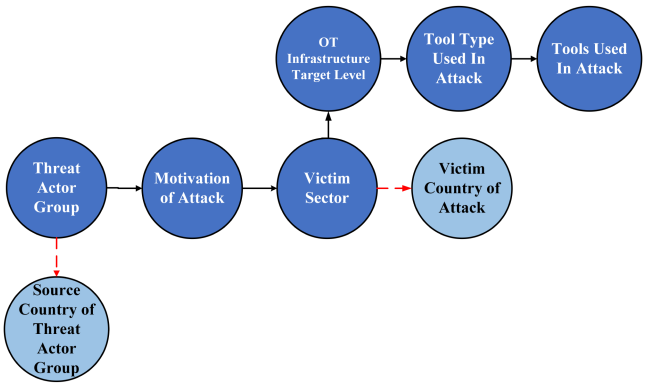

FIGURE 6. Escalation of attacks in OT environment.

Knowledge about the threat actors' *tool usage and its types* enhances actively preparing for the threat in advance by recognizing trends that may be used to attack in the future. Then, security teams can track down the indicator of compromise (IoC) associated with signature findings in the future. Then, the recognized tools help employ proactive measures to guard the structure against possible threats.

Moreover, it assists organizations in implementing appropriate measures against attacks. Security measures, such as by introducing Intrusion Detection System, Intrusion Prevention System, Security Information and Event Management, Managed Detection and Response, Endpoint Detection and Response, Extended Detection and Response, security orchestration, automation, and response, and firewalls may be programmed to prevent the application of particular tools. A few limitations that can impact these measures are the use of tools like Mimikatz, Living off the Land, and Cobalt strike, among other tools Fig. 4(b) are used. In contrast, using these tools undetected by attackers may indicate a rising number of successful attacks. Fig. 6 visually represents the interconnectedness of these critical factors and outlines the process of escalation attacks. The genesis of any high-profile attack is often rooted in the actions of threat actor groups, which, notably, lack inherent affiliation with any specific source country due to the global distribution of their members.

Each threat actor is motivated by specific factors, influencing their choice of target sectors. Notably, the location of the victim sector may not be specific to any particular country. Subsequently, the threat group strategically determines the OT infrastructure level they intend to target, employing specific tool types based on this level. The selection of tools is critical for gaining access to the targeted infrastructure.

Understanding the motivations behind attacks empowers organizations to mitigate vulnerabilities proactively. An in-depth analysis of tools enhances threat detection capabilities and facilitates the implementation of tailored countermeasures against those tools. Insights into targeted sectors, levels, and countries foster collaborative defense strategies as shown in the next Section VII.

TABLE 2. Overview of Cybersecurity Frameworks Associated With Security Measures for IT and OT Environments, Detailing Implementation Roles and Levels

Security Measures	Description	Level	Roles	IT	OT	Relevant Frameworks
Use Updated Antivirus and Antimalware Software [64], [65]	Install reputable antivirus and antimalware software on all devices and servers. Keep these applications updated to ensure they can detect and remove the latest malware threats.	Technical	Asset Owner. System Integrator	✓	✓	NIST 800-53, ISA/IEC 62443, NIS Directives
Regular Software Updates and Patching [64], [65]	Keep operating systems, applications, and software up-to-date with the latest security patches. Many malware attacks exploit known vulnerabilities in outdated software.	Technical	Asset Owner, System Integrator	✓	✓	NIST 800-53, NIST 800-82r3, ISO 27000 Series, CIS Critical Security Controls
Implement Strong Password Policies [64], [65]	Enforce strong password policies across the network to prevent unauthorized access. Use complex passwords, multi-factor authentication (MFA), and regularly update passwords.	Organizational	Asset Owner	✓		NIST 800-53, CIS Critical Security Controls, Cybersecurity Maturity Model Certification
Educate Users [64]	Train employees and users about the risks of malware, phishing, and other social engineering techniques. Teach them to recognize suspicious emails, links, and attachments.	Human	Asset Owner	✓	✓	NIST 800-53, NIST 800-82r3, Cybersecurity Maturity Model Certification
Restrict User Privileges [64], [65], [66], [67]	Limit user privileges to the minimum necessary for their job function. Users should only have access to the resources they require to perform their duties.	Organizational	Asset Owner	✓	✓	NIST 800-53, ISO 27000 Series, NERC CIP
Network Segmentation [64], [68]	Segment the network into smaller, isolated subnetworks. This helps contain malware and prevents it from spreading throughout the entire network.	Technical	System Integrator	✓	✓	NIST 800-53, ISA/IEC 62443, MITRE ATT&CK ICS Framework, TSA Pipeline-2021-02D
Regular Data Backups [64]	Maintain regular backups of critical data and store them in a secure location, preferably offline or in the cloud. In case of a malware infection, data can restored without paying ransom or losing important information.	Technical	Asset Owner	✓	✓	NIST 800-53, ISO 27000 Series, Cybersecurity Maturity Model Certification
Web Filtering and Firewalls [64], [68]	Employ web filtering and firewalls to block access to malicious websites and unauthorized network traffic. Firewalls act as a barrier between the internal network and the internet, reducing the risk of malware infiltration.	Technical	System Integrator	✓	✓	NIST 800-53, NERC CIP, ISA/IEC 62443
Email Protection [64], [65], [69]	Implement advanced email security measures, such as anti-spam filters, email authentication (Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC)), and email encryption to prevent phishing attacks and malicious email attachments.	Technical	System Intgerator	✓		NIST 800-53, NIST 800-82r3, Cybersecurity Maturity Model Certification
Monitoring and Incident Response [64]	Continuously monitor the network for signs of malware activity and establish an incident response plan. This plan should outline how to handle and contain security incidents promptly and effectively.	Organizational	Asset Owner, System Intgrator	✓	✓	NIST 800-53, NIST 800-82r3, CIS Critical Security Controls, MITRE ATT&CK ICS Framework
Secure Remote Access [64], [66], [70]	If the organization allows remote access to its network, ensure that remote connections are secured using VPNs and other encryption technologies.	Technical	Asset Owner, System Integrator	✓	✓	NIST 800-53, NISTIR 8374, Cybersecurity Maturity Model Certification
Application Whitelisting and Blacklisting [64], [71], [72]	Consider using application whitelisting to allow only approved applications to run on the systems, and use blacklisting to block known malicious software.	Technical	Asset Owner, System Integrator	✓	✓	NIST 800-53, CIS Critical Security Controls, ISA/IEC 62443
Disable Autorun [64], [65], [73]	Disable autorun and autoplay features on devices to prevent malware from spreading through removable media.	Technical	Manufacturer, Asset Owner	✓	✓	NIST 800-53, ISA/IEC 62443
Secure Mobile Devices [64], [70]	Extend security measures to mobile devices (e.g., smartphones, tablets) that connect to the network. Implement mobile device management (MDM) solutions to enforce security policies on these devices.	Technical	Asset Owner	✓		NIST 800-53, NISTIR 8374, Qatar ICS Security Standard
Regular Security Audits [64]	Conduct periodic security audits and penetration tests to identify vulnerabilities and address them proactively.	Organizational	Asset Owner, System Integrator, Manufacturer	✓	✓	NIST 800-53, ISO 27000 Series, Cybersecurity Maturity Model Certification

VII. STRATEGIES TO DEFEND AGAINST ADVERSARIES

The assertion that there are no specific measures against APTs is grounded in the reality that APTs are complex and sophisticated attacks that can adapt to existing defenses. This makes risk analysis even more important, and it necessitates a well thought and holistic security approach particularly in the OT domain [49]. There are guidelines and best practices for defending against adversaries in both IT and OT environments, however it is important to note that there is no single source for such recommendations. Actually, they are covered by multiple standards and frameworks, such as ISA/IEC 62443 [50], NIST 800-53 [51], NIST 800-82r3 [52], the ISO

27000 Series [53], CIS Critical Security Controls [54], NERC CIP [55], the NIS Directives [56], the MITRE ATT&CK ICS Framework [57], NISTIR 8374 [58], the Cybersecurity Maturity Model Certification [59], the Qatar ICS Security Standard [60], TSA Pipeline-2021-02D (SD-02D) [61], and the NCA Essential Cybersecurity Controls [62].

Table 2 presents a compilation of some of the common strategies to defend OT environments against adversarial threat groups and which standards/frameworks recommend them. It is worth noting that most recommendations apply to IT and OT alike. A well structured, layered combination can significantly strengthen an organization's cybersecurity posture (see [63] for implementation details) and enhance resilience against APTs. Well-defined roles (manufacturer, asset owner, and system integrator) further categorized by levels, organizational, technical, and human, make the responsibilities clear, bring about accountability, and enable coordination across teams. This structured approach lets each party focus on its core tasks: manufacturers secure device design, asset owners manage policies and user training, and system integrators handle technical implementations. Such clarity simplifies compliance with frameworks. Nevertheless, continuous assessment, adaptation, and employee training remain vital to counter evolving threats effectively.

VIII. CONCLUSION

In this article, we provided an analysis of threat groups operating in OT environments, trying to gain insights into the dynamic landscape of cyber threats. By examining motives, tactics, and tools employed by adversaries targeting industrial infrastructure, this study aims to enhance our understanding of potential risks. Our examination covers victim sectors, target levels, associated countries, attack motivations, and tools used by these threat groups.

In recent years, recognition of cybersecurity's importance in industry is growing, prompting increased investment in security measures and collaboration among industry, government, research, and private sectors shows the strengthening responses to OT security challenges, exemplified by initiatives, such as the ETHOS open-source platform, for sharing anonymous early OT environment threat warning information [74]. Growing innovations in anomaly detection tools-based AI and ML are enhancing threat detection capabilities in industrial settings. However, gaps persist in cybersecurity standards and regulations for ICS as standardization does not guarantee a fully secure environment [63].

Research into threat modeling and vulnerability assessments is one way to deepen understanding of OT security risks. Nevertheless, challenges remain, including reliance on outdated legacy technology, a shortage of cybersecurity professionals in OT environments, and resistance to change. This essential factor is hampering cybersecurity adoption and progress in securing the industry. To overcome these obstacles, research should take a holistic approach, considering technical, organizational, and human factors by prioritizing high-risk areas and developing adaptive security measures vital for resilient industrial cybersecurity (see also Table 2). The insights and strategies presented in this article might provide a foundation for navigating the intricate realm of OT cybersecurity.

REFERENCES

[1] S. Santos, P. Costa, and A. Rocha, "IT/OT convergence in industry 4.0 : Risks and analysis of the problems," in *Proc. IEEE 18th Iberian Conf. Inf. Syst. Technol.*, 2023, pp. 1–6.

[2] T. Sauter and C. Schwaiger, "Achievement of secure internet access to fieldbus systems," *Microprocessors Microsystems*, vol. 26, no. 7, pp. 331–339, 2002.

[3] J. Ford and H. S. Berry, "Leveling up survey of how nation states leverage cyber operations to even the playing field," in *Proc. 11th Int. Symp. Digit. Forensics Secur. (ISDFS)*, 2023, pp. 1–5.

[4] M. Benmalek, "Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges," *Internet Things Cyber- Phys. Syst.*, vol. 4, pp. 186–202, 2024.

[5] B. Bracken, "ICS ransomware danger rages despite fewer attacks," Accessed: Apr. 24, 2024. [Online]. Available: https://www.darkreading.com/ics-ot-security/ics-ransomware-rages-fewer-attacks

[6] Deloitte, "Mitigate Healthcare Cyber Threats with AI-powered Intelligence," Accessed: Apr. 24, 2024. [Online]. Available: https://www2.deloitte.com/us/en/pages/risk/solutions/elevating-healthcare-security-proactive-defense-with-ai-threat-intelligence.html

[7] A. Bécue, I. Praça, and J. Gama, "Artificial intelligence, cyber-threats and industry 4.0: Challenges and opportunities," *Artif. Intell. Rev.*, vol. 54, no. 5, pp. 3849–3886, Jun. 2021.

[8] N. Kaloudi and J. Li, "The AI-based cyber threat landscape: A survey," *ACM Comput. Surv.*, vol. 53, no. 1, pp. 1–34, Feb. 2020.

[9] J. Sengupta, S. Ruj, and S. Das Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *J. Netw. Comput. Appl.*, vol. 149, 2020, Art. no. 102481.

[10] L. Papadopoulos et al., "Protection of critical infrastructures from advanced combined cyber and physical threats: The PRAETORIAN approach," *Int. J. Crit. Infrastructure Protection*, vol. 44, 2024, Art. no. 100657.

[11] K. Zetter, "Inside the cunning, unprecedented hack of Ukraine's power grid," 2016. [Online]. Available: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[12] Industroyer' virus could bring down power networks, researchers warn, 2017. [Online]. Available: https://tinyurl.com/r7p56 vye

[13] T. Spring, "Vpnfilter malware infects 500k routers including linksys, mikrotik, netgear," 2018. [Online]. Available: https://threatpost.com/vpnfilter-malware-infects-500k-routers-including-linksys-mikrotik-netgear/132212/

[14] M. Giles, "Triton is the world's most murderous malware, and it's spreading," 2019. [Online]. Available: https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/

[15] B. Hunter and F. Gutierrez, "Ekans ransomware: A malware targeting OT ICS systems," 2020. [Online]. Available: https://www.fortinet.com/blog/threat-research/ekans-ransomware-targeting-ot-ics-systems

[16] T. W. House, "Colonial pipeline cyber incident," 2021. [Online]. Available: https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

[17] S. Hanson, "Deep dive into pipedream's OPC UA module, mousehole," 2023. [Online]. Available: https://www.dragos.com/blog/pipedream-mousehole-opcua-module/

[18] A. Lemay, J. Calvet, F. Menet, and J. M. Fernandez, "Survey of publicly available reports on advanced persistent threat actors," *Comput. Secur.*, vol. 72, pp. 26–59, 2018.

[19] Bahrami, "Cyber kill chain-based taxonomy of advanced persistent threat actors: Analogy of tactics, techniques, and procedures," *J. Inf. Process. Syst.*, vol. 15, no. 4, pp. 865–889, Aug. 2019.

[20] S. Singh, P. K. Sharma, S. Y. Moon, D. Moon, and J. H. Park, "A comprehensive study on apt attacks and countermeasures for future networks and communications: Challenges and solutions," *J. Supercomput.*, vol. 75, no. 8, p. 4543–4574, Aug. 2019.

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

[22] S. Hussain, M. B. Ahmad, and S. S. Uddin Ghouri, "Advance persistent threat—A systematic review of literature and meta-analysis of threat vectors," in *Proc. Adv. Comput. Commun. Comput. Sci.*, Singapore: Springer, 2021, pp. 161–178.

[23] M. A. Talib, Q. Nasir, A. B. Nassif, T. Mokhamed, N. Ahmed, and B. Mahfood, "APT beaconing detection: A systematic review," *Comput. Secur.*, vol. 122, 2022, Art. no. 102875.

[24] I. Kotenko, D. Gaifulina, and I. Zelichenok, "Systematic literature review of security event correlation methods," *IEEE Access*, vol. 10, pp. 43387–43420, 2022.

[25] K. Huang, M. Siegel, and S. Madnick, "Systematically understanding the cyber attack business: A survey," *ACM Comput. Surveys*, vol. 51, no. 4, pp. 1–36, Jul. 2018.

[26] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Comput. Netw.*, vol. 169, 2020, Art. no. 107094.

[27] P. Bhatt, E. T. Yano, and P. Gustavsson, "Towards a framework to detect multi-stage advanced persistent threats attacks," in *Proc. IEEE 8th Int. Symp. Serv. Oriented Syst. Eng.*, 2014, pp. 390–395.

[28] P. Giura and W. Wang, "A context-based detection framework for advanced persistent threats," in *Proc. 2012 Int. Conf. Cyber Secur.*, 2012, pp. 69–74.

[29] J. R. Johnson and E. A. Hogan, "A graph analytic metric for mitigating advanced persistent threat," in *Proc. 2013 IEEE Int. Conf. Intell. Secur. Informat.*, 2013, pp. 129–133.

[30] G. Ioannou, P. Louvieris, N. Clewley, and G. Powell, "A markov multi-phase transferable belief model: An application for predicting data exfiltration apts," in *Proc. 16th Int. Conf. Inf. Fusion*, 2013, pp. 842–849.

[31] W. Niu, X. Zhang, G. Yang, R. Chen, and D. Wang, "Modeling attack process of advanced persistent threat using network evolution," *IEICE Trans. Inf. Syst.*, vol. E 100.D, no. 10, pp. 2275–2286, 2017.

[32] S. Caltagirone, A. Pendergast, and C. Betz, "The diamond model of intrusion analysis," pp. 1–61, 2013.

[33] T. Rid and B. Buchanan, "Attributing cyber attacks," *J. Strategic Stud.*, vol. 38, no. 1/2, pp. 4–37, 2015.

[34] Y. Mei, W. Han, S. Li, X. Wu, K. Lin, and Y. Qi, "A review of attribution technical for apt attacks," in *Proc. IEEE 7th Int. Conf. Data Sci. Cyberspace*, pp. 512–518, 2022.

[35] A. Sundaram, H. S. Abdel-Khalik, and O. Ashy, "A data analytical approach for assessing the efficacy of operational technology active defenses against insider threats," *Prog. Nucl. Energy*, vol. 124, 2020, Art. no. 103339.

[36] C. Krasznay and G. Gyebnár, "Possibilities and limitations of cyber threat intelligence in energy systems," in *Proc. 13th Int. Conf. Cyber Conflict*, 2021, pp. 171–188.

[37] Z. Jadidi and Y. Lu, "A threat hunting framework for industrial control systems," *IEEE Access*, vol. 9, pp. 164118–164130, 2021.

[38] "All groups - threat group cards: A threat actor encyclopedia," Accessed: Jul. 26, 2023. [Online]. Available: https://apt.etda.or.th/cgi-bin/listgroups.cgi

[39] F. Fkie, "Malpedia fraunhofer FKIE," Accessed: Jul. 26, 2023. [Online]. Available: https://malpedia.caad.fkie.fraunhofer.de/

[40] "Groups | MITRE ATT&CK," Accessed: Jul. 26, 2023. [Online]. Available: https://attack.mitre.org/groups/

[41] "Cybersecurity alerts & advisories| CISA," Accessed: Jul. 26, 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories

[42] M. P. Bhole, "Data analysis and results of threat groups in OT environment," 2023. [Online]. Available: https://researchdata.tuwien.at/records/ewmb8-3ad52

[43] "Enterprise-control system integration–part 1: Models and terminology," in *Proc. Int. Soc. Automat.*, 2010.

[44] T. Yadav and A. M. Rao, "Technical aspects of cyber kill chain," in *Security in Computing and Communications*, J.H. Abawajy, S. Mukherjea, S. M. Thampi, and A. Ruiz-Martínez, eds. Cham: Berlin, Germany: Springer, 2015, pp. 438–452.

[45] M. J. Assante and R. M. Lee, "The industrial control system cyber kill chain," 2016, [Online]. Available: https://api.semanticscholar.org/CorpusID, pp 213190869

[46] R. Lakshmanan, "Here's how solarwinds hackers stayed undetected for long enough," 2021. [Online]. Available: https://thehackernews.com/2021/01/heres-how-solarwinds-hackers-stayed.html

[47] A. Kling and P. Forney, "Triton - schneider electric analysis and disclosure," (n.d.). [Online]. Available: https://www.youtube.com/watch?v=f09E75bWvkk

[48] B. Johnson, D. Caban, M. Krotofil, D. Scali, N. Brubaker, and C. Glyer, "Attackers deploy new ICS attack framework "triton" and cause operational disruption to critical infrastructure," 2017. [Online]. Available: https://www.mandiant.com/resources/blog/attackers-deploy-new-ics-attack-framework-triton

[49] S. Hollerer, T. Sauter, and W. Kastner, "Risk assessments considering safety, security, and their interdependencies in OT environments," in *Proc. 17th Int. Conf. Availability, Rel. Secur.*, 2022, pp. 1–8.

[50] *ISA/IEC 62443: Secur. for Ind. Automat. and Control Syst., Int. Soc. of Automat. (ISA), Int. Electrotechnical Commission (IEC) Std.*, 2007-2022, standards series.

[51] J. T. Force and T. Initiative, "Security and privacy controls for federal information systems and organizations (NIST SP 800-53 revision 5)," Tech. Rep. 53, Sep. 2020.

[52] K. Stouffer et al., "Guide to operational technology (ot) security (nist sp 800-82 revision 3)," Tech. Rep. 82, 2023.

[53] *ISO/IEC 27000 Series: Information Security Management Systems, International Organization for Standardization (ISO), International Electrotechnical Commission (IEC)* Std., 2005-present, standards series.

[54] Center for Internet Security, "CIS critical security controls version 8.1," Tech. Rep., Jun. 2024. [Online]. Available: https://www.cisecurity.org/controls/v8-1

[55] *NERC Critical Infrastructure Protection (CIP) Standards, North American Electric Reliability Corporation (NERC) Std.*, 2018-2021, *standards series*.

[56] European Union, "Directive (EU) 2016/1148 on security of network and information systems (NIS directive)," 2016. [Online]. Available: https://eur-lex.europa.eu/ legal-content/EN/TXT/?uri=CELEX:32016L1148

[57] O. Alexander, M. Belisle, and J. Steele, "MITRE ATT&CK for industrial control systems: Design and philosophy," 2020.

[58] W. C. Barker, W. Fisher, K. Scarfone, and M. Souppaya, "Ransomware risk management: A cybersecurity framework profile," Nat. Inst. Stand. Technol. (USA), Tech. Rep., Feb. 2022. [Online]. Available: http://dx.doi.org/10.6028/NIST.IR.8374

[59] "Cybersecurity maturity model certification (CMMC) 2.0" U.S. Department of Defense, 2021. [Online]. Available: https://www.acq.osd.mil/cmmc/

[60] *Qatar ICS Security Standard, Qatar Ministry of Interior Std.*, 2017, industry standard.

[61] "TSA aecurity directive pipeline-2021-02D (SD-02D)" U. S. Transportation Security Administration (TSA), 2021, pipeline cybersecurity security directive.

[62] *Nat. Cybersecurity Authority (NCA) Essential Cybersecurity Controls (ECC)*, "National cybersecurity authority, kingdom of Saudi Arabia std., 2018. [Online]. Available: https://nca.gov.sa

[63] M. Bhole, W. Kastner, and T. Sauter, "From manual to semi-automated safety and security requirements engineering: Ensuring compliance in industry 4.0," in *Proc. IEEE 50th Annu. Conf. Ind. Electron. Soc.*, Chicago, Illinois, USA, 2024, pp. 749–754.

[64] "Bundesamt für sicherheit in der informationstechnik - recommendations," Accessed: Aug. 08, 2023. [Online]. Available: https://tinyurl.com/BSIRecommendations

[65] K. Scarfone, "NIST special publication (SP) 800-83 rev. 1, guide to malware incident prevention and handling for desktops and laptops," Accessed: Aug. 04, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/83/r1/final

[66] P. A. Grassi, M. E. Garcia, and J. L. Fenton, "Digital identity guidelines," Accessed: Aug. 08, 2023. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

[67] D. Walkowski, "What is the principle of least privilege and why is it important?," Accessed: Aug. 08, 2023. [Online]. Available: https://www.f5.com/labs/learning-center/what-is-the-principle-of-least-privilege-and-why-is-it-important

[68] Praveen, "Six best practices for secure network firewall configuration," Accessed: Aug. 04, 2023. [Online]. Available: https://www.eccouncil.org/cybersecurity-exchange/network-security/six-network-firewall-configuration-best-practices/

[69] "How DMARC advances email security," Accessed: Aug. 04, 2023. [Online]. Available: https://www.cisecurity.org/insights/blog/how-dmarc-advances-email-security

[70] S. Karen, "NIST special publication (SP) 800-46 Rev. 2, guide to enterprise telework, remote access, and bring your own device (BYOD) security," Accessed: Aug. 04, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/46/r2/final
[71] "What Is Endpoint Security? How It Works & Its Importance," Accessed: Aug. 04, 2023. [Online]. Available: https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-security.html#::text=EPPs%20secure%20endpoints%20through%20application,which%20helps%20prevent%20data%20loss
[72] K. Scarfone, "NIST special publication (SP) 800-61 rev. 2, computer security incident handling guide," Accessed: Aug. 04, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/61/r2/final
[73] "Using caution with USB drives| CISA," Accessed: Aug. 04, 2023. [Online]. Available: https://www.cisa.gov/news-events/news/using-caution-usb-drlives
[74] "ETHOS | emerging threat open sharing — ethos-org.io," Accessed: Jul. 23, 2024. [Online]. Available: https://www.ethos-org.io/

MUKUND BHOLE received the B.Tech degree in information technology from Shivaji University, Kolhapur, India, in 2019, and the M.Tech degree in information security from COEP Technological University, Pune, India, in 2021. He is currently working toward the Ph.D. degree with Technische Universität Wien, Vienna, Austria.

His research focus on safety and security in operational technology environments. In addition, he serves as a Project Assistant with #SafeSecLab. His research interests include information security, penetration testing, intrusion detection, vulnerability assessment, and overall industrial cybersecurity.

THILO SAUTER (Fellow, IEEE) received the Dipl.-Ing. and Ph.D. degrees in electrical engineering from Vienna University of Technology, Vienna, Austria, in 1992 and 1999, respectively.

He is a Professor for automation technology with TU Wien, Vienna, Austria, as well as Senior Scientist with the University of Continuing Education Krems, Wiener Neustadt, Austria. From 2004 to 2013, he also was the Founding Director of the Institute for Integrated Sensor Systems with the Austrian Academy of Sciences. His expertise and research interests include embedded systems and integrated circuit design, smart sensors, and automation and sensor networks with a focus on real-time, security, interconnection, and integration issues relevant to cyber-physical systems and the Internet of Things in various application domains such as industrial and building automation, smart manufacturing, or smart grids.

Dr. Sauter is Member of the Board of the Austrian Electrotechnical Association and Senior AdCom Member of the IEEE Industrial Electronics Society. Moreover, he has been involved in the standardization of industrial communication systems for more than 25 years.

WOLFGANG KASTNER (Senior Member, IEEE) received the Dipl.-Ing. and Dr.Techn. degrees in computer science from the Vienna University of Technology, Vienna, Austria, in 1992 and 1996, respectively.

He is currently a Full Professor of the Industrial Internet of Things with the Faculty of Informatics, Technische Universität Wien, Vienna, Austria. His research addresses distributed automation and (industrial) communication systems in various application domains, such as factory automation, building automation, and smart grids. His research topics tackle the safe while secure IT/OT convergence and approaches for the Industrial Internet based on information modeling and knowledge representation.