GSC Advanced Research and Reviews

eISSN: 2582-4597 CODEN (USA): GARRC2

Cross Ref DOI: 10.30574/gscarr

Journal homepage: https://gsconlinepress.com/journals/gscarr/

(REVIEW ARTICLE)

Check for updates

Botnets and Critical Infrastructure Security: A Survey

Hallowe Andrew *

Jaramogi Oginga Odinga University of Science and Technology.

GSC Advanced Research and Reviews, 2025, 22(01), 330-361

Publication history: Received on 10 October 2024; revised on 22 January 2025; accepted on 25 January 2025

Article DOI: https://doi.org/10.30574/gscarr.2025.22.1.0445

Abstract

Botnets have emerged as a significant threat to the security and resilience of critical infrastructure systems. These decentralized networks of compromised devices enable malicious actors to execute sophisticated cyberattacks, such as Distributed Denial of Service (DDoS) attacks, data exfiltration, and ransomware deployment, which can disrupt essential services and compromise national security. This paper examines the evolving landscape of botnet threats to critical infrastructure, highlighting the vulnerabilities inherent in increasingly interconnected systems, including industrial control systems (ICS), smart grids, and healthcare networks. It explores how advancements in artificial intelligence (AI), machine learning (ML), and the Internet of Things (IoT) have expanded the attack surface for botnets while also offering potential mitigation strategies. Furthermore, the paper reviews contemporary defense mechanisms, including anomaly detection, threat intelligence sharing, and network segmentation, and assesses their efficacy in safeguarding critical infrastructure. By identifying gaps in existing security frameworks and proposing a multi-layered, proactive defense approach, this study aims to enhance the resilience of critical infrastructure against botnet-driven threats. The findings underscore the urgent need for collaboration between policymakers, industry stakeholders, and cybersecurity experts to develop robust and adaptive solutions in the face of this escalating cyber threat.

Keywords: Bots; Botnet; Security; Critical Infrastructure; Performance

1. Introduction

Critical infrastructure, defined as the essential systems and assets that underpin the functioning of society, plays a vital role in maintaining economic stability, public health, and national security [1], [2]. These infrastructures include sectors such as energy, transportation, water management, financial services, and healthcare. As technological advancements drive the digital transformation of these systems, they become increasingly interconnected, automated, and reliant on networked devices [3], [4]. While these changes have improved efficiency and functionality, they have also significantly expanded the attack surface for cyber threats [6]. Among the most prominent and disruptive of these threats are botnets.

Botnets are networks of compromised devices, ranging from personal computers to industrial Internet of Things (IoT) devices [6], that are remotely controlled by a central operator. Often created through the exploitation of vulnerabilities or malware infection, these networks are used for a variety of malicious purposes, including Distributed Denial of Service (DDoS) attacks, data exfiltration, ransomware distribution, and the propagation of additional malware [7]-[11]. Their distributed nature and the increasing ubiquity of vulnerable connected devices make botnets a formidable challenge in cybersecurity.

The intersection of botnet threats and critical infrastructure security has become a pressing concern for governments, industry stakeholders, and cybersecurity researchers [12], [13]. Critical infrastructure systems are increasingly dependent on interconnected technologies, such as Industrial Control Systems (ICS), Supervisory Control and Data

* Corresponding author: Hallowe Andrew.

Acquisition (SCADA) systems, and IoT devices [14], [15]. These technologies, while transformative, often operate with legacy hardware and software that lack modern security protections. Furthermore, the interdependencies between critical infrastructure sectors amplify the risks: an attack on one system, such as a power grid, can trigger cascading failures across healthcare, transportation, and financial systems [16].

Several high-profile cyberattacks have highlighted the potential for botnets to disrupt critical infrastructure. For example, the Mirai botnet demonstrated how IoT devices could be weaponized to launch large-scale DDoS attacks, temporarily crippling major internet services [17]-[20]. More recently, the emergence of sophisticated botnets leveraging artificial intelligence (AI) and machine learning (ML) capabilities [21] has underscored the growing complexity and scale of the threat landscape. As attackers innovate, traditional defenses often struggle to keep pace, leaving critical infrastructure systems vulnerable to exploitation [22], [23]. This paper seeks to address the multifaceted challenge of botnets in the context of critical infrastructure security. The objectives of this research are threefold:

- *Threat assessment*: To analyze the evolving nature of botnets, their capabilities, and their potential impact on critical infrastructure systems. This includes examining the role of emerging technologies, such as AI, in enhancing the sophistication of botnet operations.
- *Defense strategies*: To evaluate the effectiveness of existing security measures, including threat detection systems, network segmentation, and incident response frameworks, in mitigating botnet-driven risks to critical infrastructure.

The paper is organized as follows. Section 2 provides a detailed overview of botnet architecture, including the methods used for their creation, propagation, and operation. Section 3 explores the vulnerabilities in critical infrastructure systems and the specific risks posed by botnets. Section 4 dscribes some of the notable botnet threats while Section 5 describes performance challenges occasioned by botnets. On the other hand, Section 6 reviews existing defense mechanisms and highlights the limitations of current approaches. Section 7 discusses emerging technologies and strategies for enhancing resilience against botnet-driven attacks. Finally, Section 8 offers conclusions and recommendations for future research.

2. Botnet architecture

Botnet architecture refers to the structural design and operational framework that enables the creation, control, and execution of botnet activities [24], [25]. As shown in Figure 1, a botnet comprises multiple compromised devices, known as bots or zombies, which are infected with malware and controlled remotely by a botmaster or bot herder. These devices can range from personal computers and servers to Internet of Things (IoT) devices and smartphones. At the core of a botnet is the Command and Control (C2) infrastructure, which serves as the communication hub for issuing commands to bots and receiving feedback or stolen data. The botmaster utilizes this infrastructure to coordinate malicious activities [26] such as DDoS attacks, data theft, spamming, or ransomware deployment.

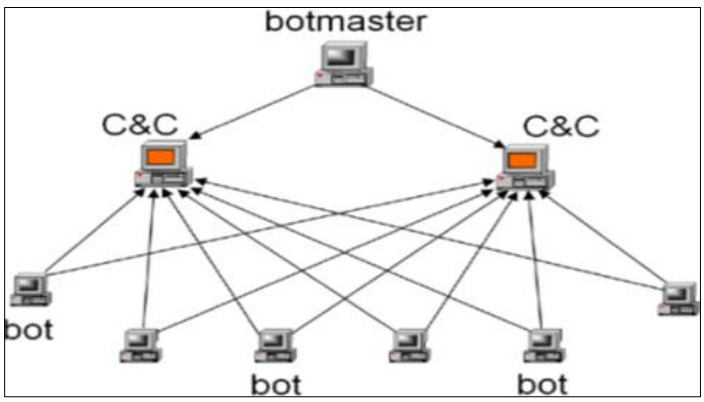

Figure 1 A botnet

Botnets can follow different communication models, with the choice of architecture affecting their scalability, resilience, and detectability [27], [28]. In a centralized architecture, bots connect directly to one or more C2 servers, making the system easier to control but vulnerable to disruption if the C2 server is identified and taken down [29]. Conversely, decentralized or peer-to-peer (P2P) botnets distribute command communication across the bots themselves, eliminating a single point of failure and enhancing resilience, albeit at the cost of increased complexity [30], [31]. Hybrid

architectures, which combine centralized and decentralized models, offer a balance between control efficiency and resilience, enabling the botnet to adapt dynamically to defensive measures [32].

The C2 communication channels play a crucial role in botnet operation, influencing both their functionality and ability to evade detection [33], as shown in Figure 2. Common channels include HTTP/HTTPS, which blend seamlessly with legitimate web traffic; DNS-based communication, often employing domain generation algorithms (DGA) to dynamically alter C2 server addresses; and emerging platforms such as social media and encrypted messaging services [34], [35]. Some botnets use custom protocols to further obfuscate their communication patterns, complicating detection efforts. To maintain their stealth and longevity, botnets frequently employ techniques like encryption [36] of C2 traffic, fast-flux to rapidly change IP addresses, and polymorphic malware that alters its signature to evade antivirus software.

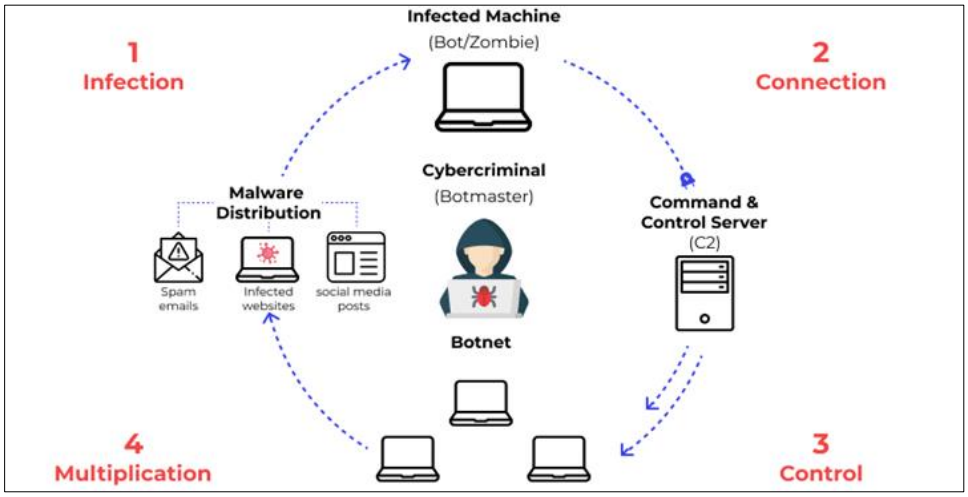

Figure 2 Botnet operation

The lifecycle of a botnet typically begins with the recruitment and infection of vulnerable devices through exploits, phishing campaigns, or malicious software [37], [38]. Once compromised, these devices are registered with the C2 infrastructure and await commands from the botmaster. The botnet then executes its malicious objectives, which may include disrupting critical services, stealing sensitive information, or propagating itself to expand the network [39], [40]. To sustain operations, botmasters continuously update their malware, switch C2 servers, and employ strategies like domain fluxing to avoid detection and takedown efforts.

As botnets evolve, they are increasingly leveraging advancements in artificial intelligence, machine learning [41], and blockchain technologies to enhance their capabilities and resilience. Understanding the underlying architecture of botnets is critical for developing effective cybersecurity measures to mitigate their impact [42], particularly in the context of critical infrastructure, where disruptions can have far-reaching consequences. By dissecting their design and communication patterns, cybersecurity professionals can identify vulnerabilities within botnets and devise strategies to neutralize their threats effectively.

3. Botnets and critical infrastructure security

Critical infrastructure—encompassing sectors such as energy, transportation, water systems, healthcare, and finance—is vital to the functioning of modern society [43], [44]. These systems are increasingly digitized, interconnected, and reliant on complex networked devices, making them attractive and vulnerable targets for cyber threats. Botnets, which are networks of compromised devices remotely controlled by malicious actors, pose a significant threat to the security and resilience of critical infrastructure [45]. Their ability to launch coordinated and large-scale attacks can result in operational disruptions, economic losses, and even endanger public safety. The sub-sections below describe the multifaceted effects of botnets on critical infrastructure security in detail.

3.1. Operational disruption

Botnets can disrupt the operations of critical infrastructure through attacks such as DDoS. By overwhelming servers, routers, or communication networks with massive volumes of traffic, botnets can render systems unavailable, causing widespread outages [47]-[50]. For instance, an attack on the control systems of an electric grid can result in power

outages, which in turn affect healthcare facilities, transportation systems, and emergency services [51]. Similarly, disruptions in water management systems can compromise water supply and sanitation, endangering public health. These operational disruptions highlight the cascading effects botnet attacks can have on interconnected infrastructure sectors.

3.2. Data breaches and information theft

Critical infrastructure systems often manage sensitive and confidential data, including personal information, operational blueprints, and real-time monitoring data [52], [53]. Botnets can facilitate large-scale data breaches by infiltrating networks and exfiltrating valuable data. For example, an attacker could use a botnet to access a hospital's database, stealing patient records or disrupting medical device functionality. In the financial sector, botnets can compromise customer data or facilitate unauthorized transactions, leading to financial losses and reputational damage [54]-[56]. Such breaches undermine public trust in critical services and can have legal and regulatory repercussions for infrastructure operators.

3.3. Propagation of malware and ransomware

Botnets are commonly used to distribute malware, including ransomware, to critical infrastructure systems [57]. Ransomware encrypts operational data or systems, rendering them unusable until a ransom is paid. Critical infrastructure entities are particularly susceptible to ransomware attacks because their operations are time-sensitive and essential to societal functions [58]-[60]. For instance, a ransomware attack on a hospital could delay critical treatments, while one on a transportation network could paralyze logistics and supply chains [61]. The Colonial Pipeline attack in 2021 is a prominent example where ransomware disrupted fuel supply across several states, underscoring the vulnerability of infrastructure to botnet-enabled malware.

3.4. Manipulation of Industrial Control Systems (ICS)

The ICS are integral to the functioning of critical infrastructure, enabling automation and control of processes in energy plants, manufacturing, and water systems [62], [63]. Botnets targeting ICS can manipulate system parameters, disrupt operations, or cause physical damage to infrastructure. For example, a botnet could alter the flow rates in a water treatment facility, compromising water quality, or disrupt the synchronization of power grids, leading to blackouts [64]-[66]. The Stuxnet worm, though not a botnet, demonstrated how cyberattacks on ICS can cause real-world consequences, serving as a cautionary example for botnet-related threats.

3.5. Economic and financial impacts

The economic repercussions of botnet attacks on critical infrastructure can be severe [67]. Operational downtime, repair costs, data recovery efforts, and lost revenue during service outages can amount to significant financial losses. Furthermore, the cost of enhancing security measures post-attack and addressing regulatory compliance can strain budgets [68], [69]. For example, botnet-enabled DDoS attacks on financial institutions can halt transactions and undermine confidence in banking systems, potentially destabilizing local or even national economies.

3.6. Undermining national security

Critical infrastructure systems are often considered strategic assets due to their role in national security [70]. Botnet attacks on these systems can have geopolitical implications, particularly when state-sponsored actors or advanced persistent threats (APTs) are involved. For instance, an attack on a country's energy grid [71] or transportation networks during a period of political tension could weaken its response capabilities and destabilize its economy. Such attacks can also serve as a precursor to larger-scale cyber warfare [72], making botnets a significant concern for national defense agencies.

3.7. Exploitation of IoT devices

The proliferation of IoT devices in critical infrastructure has expanded the attack surface for botnets [73]. IoT devices, often deployed in monitoring and control systems, are frequently under-secured and lack proper patching mechanisms [74], [75]. Botnets often exploit IoT devices due to their widespread adoption, limited security measures, and ease of compromise. Many IoT devices, such as cameras, routers, and smart home appliances, come with weak default passwords, outdated firmware, and minimal built-in security, making them vulnerable to exploitation [76]. As shown in Figure 3, cybercriminals can scan the internet for unsecured IoT devices, using automated tools to exploit known vulnerabilities or brute-force weak credentials to gain unauthorized access [77], [78]. Once compromised, these devices become part of a botnet, often without the user's knowledge, and can be used to launch large-scale DDoS attacks, spread

malware, or steal sensitive data. The sheer number of interconnected IoT devices, many of which are inadequately secured, has made them a prime target for botnet operators seeking to amplify their reach and impact.

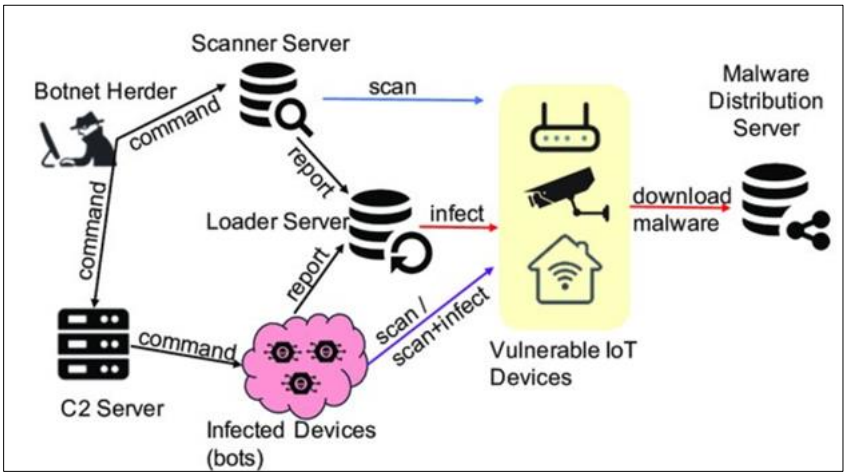

Figure 3 Botnets in IoT devices

Botnets, like the Mirai botnet, exploit these vulnerabilities to recruit IoT devices [79], amplifying their scale and impact. For example, IoT devices in smart grids, traffic management systems, or healthcare facilities can be hijacked to disrupt operations or launch further attacks, compounding the risks to critical infrastructure.

3.8. Cascading effects and interdependencies

Critical infrastructure sectors are highly interdependent [80], meaning an attack on one sector can cascade into others. For instance, a botnet attack on the energy sector can affect transportation systems reliant on electric power, disrupt water treatment facilities, and impair communication networks [81]-[83]. Such cascading effects can amplify the impact of botnet attacks, making recovery more complex and prolonging disruptions. The interconnected nature of modern infrastructure systems amplifies the risk and requires holistic approaches to security.

3.9. Undermining public trust

Repeated or high-profile botnet attacks on critical infrastructure can erode public confidence in the reliability and safety of essential services [84]. For instance, frequent power outages due to botnet attacks on the energy sector can lead to societal unrest, economic stagnation, and reduced faith in government and private sector operators. Public trust is essential for the smooth functioning of critical infrastructure [85], and its erosion can have long-term consequences for societal stability.

3.10. Challenges in detection and response

Botnets often use sophisticated evasion techniques such as encryption [86], polymorphic malware, and fast-flux DNS to avoid detection. These techniques can delay response efforts, allowing attacks to persist longer and cause more damage [87]. Furthermore, the distributed nature of botnets complicates attribution, making it challenging to identify and hold perpetrators accountable [88]. The dynamic evolution of botnets requires critical infrastructure operators to adopt advanced detection tools and robust incident response frameworks [89], which can be resource-intensive and technically demanding.

4. Notable botnet attacks on critical infrastructure

Botnets pose a significant and multifaceted threat to critical infrastructure security. Their potential to disrupt operations, compromise sensitive data, and cause cascading failures across interconnected systems underscores the need for proactive and comprehensive cybersecurity measures [90], [91]. Addressing these threats requires collaboration among governments, industry stakeholders, and cybersecurity experts to enhance resilience, detect emerging threats, and respond effectively to incidents. As the sophistication of botnets continues to grow, protecting critical infrastructure from their effects must remain a top priority to safeguard societal stability and national security. Botnet attacks have increasingly targeted critical infrastructure sectors such as energy, transportation, finance, and

healthcare [92], [93]. These attacks exploit the vulnerabilities in complex, interconnected systems to disrupt services, steal data, or demand ransom.

4.1. Mirai Botnet

The Mirai botnet, first discovered in 2016, is one of the most notorious and impactful botnets to date, primarily leveraging compromised IoT devices such as security cameras, routers, and DVRs [94]. Mirai scans the internet for devices with weak or default login credentials and then infects them by exploiting these vulnerabilities [95]. Once compromised, the devices are enslaved into a botnet, which is then used to execute massive DDoS attacks, overwhelming target websites or servers with high volumes of traffic. The most notable attack orchestrated by Mirai was against the Dyn DNS provider, which disrupted major websites, including Twitter, Netflix, and Reddit. The Mirai botnet's widespread impact brought global attention to the security risks posed by poorly protected IoT devices [96] and highlighted the need for stronger security protocols in the Internet of Things ecosystem. The Mirai botnet is one of the most infamous botnet attacks, targeting IoT devices such as routers, cameras, and DVRs [97], [98]. In 2016, it was used to launch massive Distributed Denial of Service (DDoS) attacks against DNS provider Dyn.

- *Impacts:* The attack caused widespread outages, affecting services like Twitter, Netflix, PayPal, and Reddit [99]. Although not directly targeting traditional critical infrastructure, the attack highlighted the vulnerabilities of IoT devices and their cascading effects on internet-dependent systems.
- *Prevention*: The Mirai botnet underscored the need for stronger security measures for IoT devices and the importance of robust DNS infrastructure in ensuring service continuity. As shown in Figure 4, detecting the Mirai botnet involves identifying its unique patterns of behavior, network traffic, and signature-based characteristics. Since Mirai primarily targets IoT devices by exploiting weak or default credentials, one detection approach is to monitor authentication logs for repeated failed login attempts, indicative of brute-force attacks. Network traffic analysis [100] is another key method, focusing on unusual spikes in outbound requests or scanning activities directed at other IoT devices, which are hallmarks of Mirai's propagation phase.

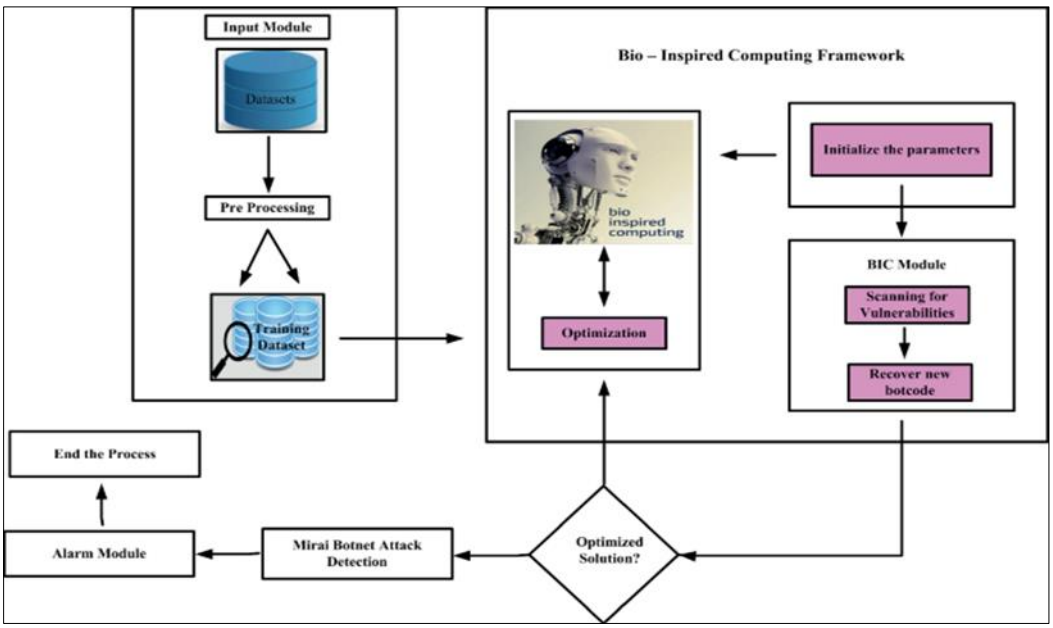

Figure 4 Mirai detection

Additionally, Intrusion Detection Systems (IDS) can use known signatures of Mirai's payloads and communication patterns with its command-and-control (C&C) servers to flag suspicious activity. Behavioral analysis tools can also detect anomalies in IoT devices, such as unexpected increases in resource usage [101] or abnormal communication with external servers. Effective Mirai detection requires a combination of these techniques, deployed in real-time to identify and mitigate botnet activity before it results in large-scale DDoS attacks.

4.2. BlackEnergy attack on Ukraine power grid

The BlackEnergy attack on Ukraine's power grid, which occurred in December 2015, was a sophisticated cyberattack that targeted the country's electrical infrastructure, causing widespread power outages [102]. The attack, attributed to

Russian state-sponsored cybercriminal group Sandworm, used the BlackEnergy malware to infiltrate the systems of three regional electricity distribution companies [103]. Once inside, the attackers gained control over supervisory control and data acquisition (SCADA) systems, disabling key components of the grid's operations. The malware allowed the attackers to remotely shut down substations, cut off power, and disrupt electrical services for several hundred thousand people. Additionally, the attack involved the use of malicious code to erase data from the control systems, complicating recovery efforts [104]. The BlackEnergy attack was a groundbreaking example of cyber warfare targeting critical infrastructure, highlighting the vulnerability of power grids to cyber threats and the potential for widespread societal and economic disruption.

- *Impact:* The attack left approximately 225,000 people without electricity for several hours [105]. It demonstrated how botnets could exploit ICS vulnerabilities to disrupt critical infrastructure operations.
- *Prevention*: This attack highlighted the vulnerability of energy infrastructure to cyber threats and emphasized the importance of securing ICS and SCADA systems against advanced botnet attacks.

4.3. WannaCry ransomware

WannaCry was a widespread ransomware attack that emerged in May 2017, exploiting a vulnerability in Microsoft Windows systems known as EternalBlue [106], which was believed to have been stolen from the U.S. National Security Agency (NSA). The ransomware rapidly spread across networks, encrypting files on infected computers and demanding a ransom payment in Bitcoin for their decryption, as shown in Figure 5. WannaCry targeted primarily older, unpatched versions of Windows, especially affecting organizations that had failed to apply critical security updates. The attack impacted hundreds of thousands of computers across over 150 countries, disrupting industries such as healthcare [107], transportation, and telecommunications. Notably, the UK's National Health Service (NHS) was severely affected, with hospitals forced to cancel appointments and surgeries. While a security researcher inadvertently discovered a "kill switch" that slowed the spread of WannaCry, the attack highlighted the devastating potential of ransomware and the importance of timely software updates and cybersecurity preparedness. While technically not a traditional botnet, WannaCry ransomware spread through networks using botnet-like techniques [108].

- *Impact:* The UK's National Health Service (NHS) was significantly affected, with hospitals and clinics losing access to patient records, causing delays in treatment. Other sectors, including transportation and finance, experienced disruptions as well.
- *Prevention*: The attack emphasized the need for timely software patching and better network segmentation to limit the spread of malware across critical systems.

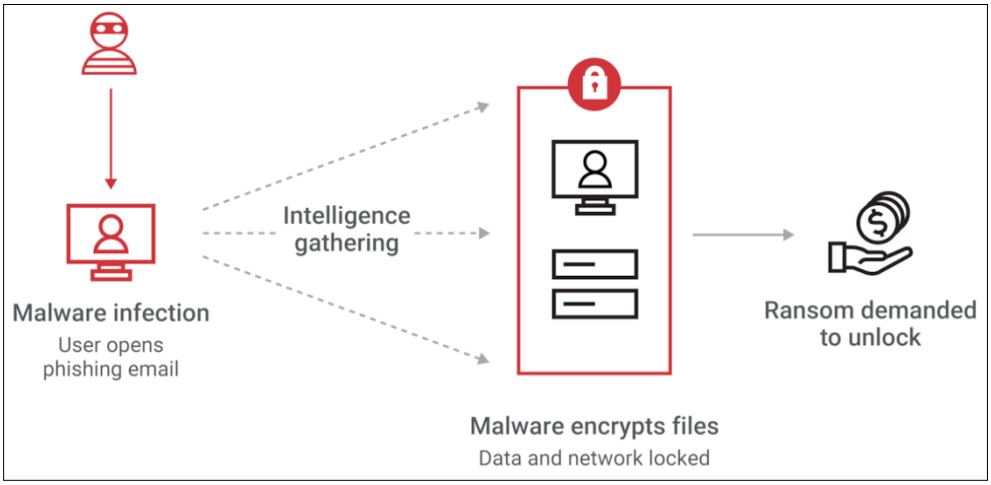

Figure 5 WannaCry ransomware

Preventing WannaCry ransomware requires a multi-layered approach focused on mitigating vulnerabilities and strengthening cybersecurity practices. The most critical step is to ensure all systems are updated with the latest security patches, particularly for vulnerabilities like EternalBlue, which WannaCry exploited [109]. Organizations should implement robust endpoint protection solutions, including antivirus software capable of detecting and blocking ransomware behavior. Network segmentation can limit the spread of malware within an organization, while regular data backups ensure that encrypted files can be restored without paying the ransom. Employing firewalls and intrusion detection/prevention systems (IDS/IPS) can help monitor and block malicious traffic [110]. Additionally, educating

employees about phishing scams and avoiding malicious email attachments or links is essential to minimize the risk of infection. Using strong, unique passwords and implementing multi-factor authentication (MFA) can further reduce vulnerabilities that ransomware like WannaCry might exploit. These preventative measures collectively help safeguard systems against similar attacks in the future.

4.4. IoTroop Botnet

The IoTroop botnet, also known as Reaper, emerged in 2017 and is a sophisticated IoT-based botnet that exploits a wide range of vulnerabilities in Internet of Things (IoT) devices [111]. As shown in Figure 6, unlike other botnets, IoTroop does not rely on default or weak passwords but instead takes advantage of known security flaws [112] in devices such as routers, cameras, and smart home products, using exploits from the likes of the Mirai botnet and additional vulnerabilities. Once compromised, these devices are used to launch DDoS attacks, send spam emails, and perform other malicious activities [113]. The IoTroop botnet is notable for its ability to evolve and adapt, with its creators using a modular architecture to easily add new exploits, making it more resilient than previous botnets [114]. It demonstrated the increasing complexity and threat of IoT-based botnets, underscoring the importance of securing connected devices against emerging cyber threats.

- *Impact:* While the full-scale impact of IoTroop on critical infrastructure remains speculative, its ability to infiltrate and control IoT devices posed a severe risk to sectors relying on IoT systems, such as smart grids and transportation.
- *Prevention*: IoTroop highlighted the growing sophistication of botnets targeting IoT devices and the need for comprehensive IoT security protocols.

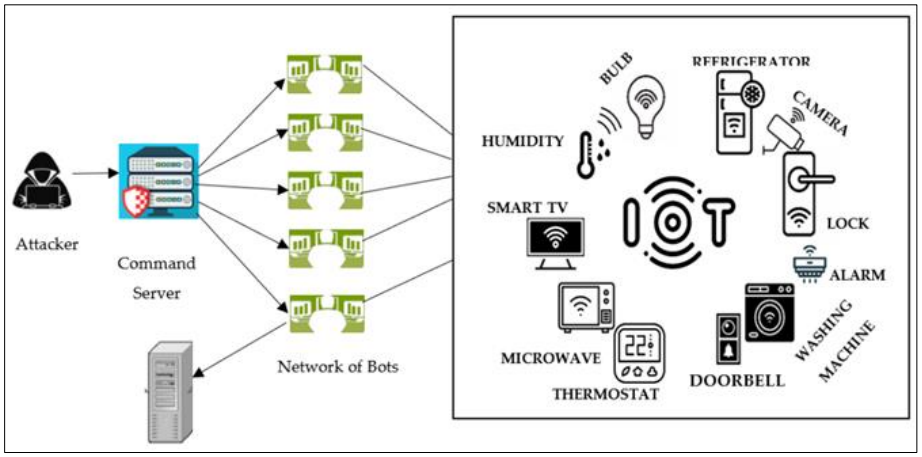

Figure 6 IoTroop botnet

Preventing the IoTroop botnet requires a proactive approach to securing Internet of Things (IoT) devices and networks. Organizations and individuals should ensure all IoT devices are updated with the latest firmware to patch known vulnerabilities that IoTroop exploits [115]. Default usernames and passwords must be changed to strong, unique credentials to prevent unauthorized access. Implementing network segmentation can isolate IoT devices from critical systems, limiting the spread of potential infections. Firewalls and intrusion detection/prevention systems (IDS/IPS) can help monitor network traffic for signs of IoTroop activity, such as exploit attempts or anomalous scanning behaviors. Regular vulnerability assessments and penetration testing can identify and address weak points in the IoT ecosystem [116]. Additionally, adopting secure device configurations, disabling unnecessary services, and using encrypted communication protocols [117] further enhance defenses. Promoting adherence to IoT security best practices at the device manufacturing level is also critical to reducing the overall attack surface and mitigating the risks posed by botnets like IoTroop.

4.5. Emotet Botnet

The Emotet botnet, initially discovered in 2014, started as a banking Trojan but evolved into one of the most prolific and dangerous malware networks, primarily used for spreading other types of malware, including ransomware and information stealers [118]. As demonstrated in Figure 7, Emotet operates by infecting victims through phishing emails that contain malicious attachments or links, often masquerading as legitimate communication from trusted entities. Once inside a network, it spreads laterally to other devices, using techniques like credential dumping and exploiting

vulnerabilities to further propagate [119]. The botnet's modular design allows it to deliver additional payloads, such as the TrickBot malware, which can then be used to steal sensitive information, install ransomware, or create backdoors. Emotet's infrastructure is highly resilient, with operators using fast-flux techniques to disguise their locations and evade detection [120]. In early 2021, a coordinated international law enforcement effort led to the takedown of Emotet's command-and-control servers, significantly disrupting its operations, though the botnet's legacy and its tactics continue to influence modern cybercriminal activities.

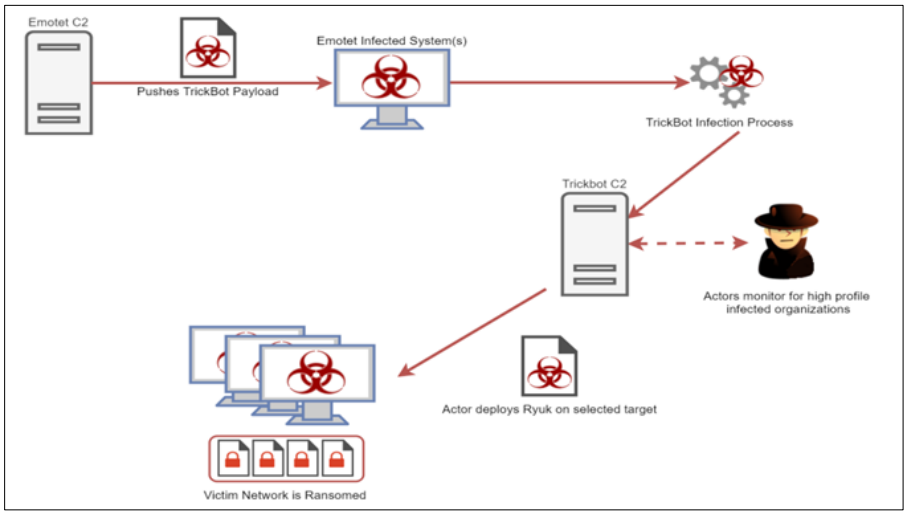

Figure 7 Emotet botnet

- *Impact:* The botnet disrupted healthcare operations by infecting systems with ransomware, causing delays in patient care. In some cases, financial systems were compromised, resulting in financial theft and operational disruptions.
- *Prevention*: Preventing the Emotet botnet requires a combination of robust cybersecurity measures, user awareness, and proactive network defenses. Since Emotet primarily spreads through phishing emails, organizations should implement advanced email filtering systems to block malicious attachments and links [121]. Educating users about recognizing phishing attempts is equally critical, as human error often facilitates its entry. Keeping all systems and software updated with the latest security patches can mitigate vulnerabilities that Emotet exploits for lateral movement. Endpoint detection and response (EDR) solutions can help identify and contain Emotet's malicious activities in real time. Network segmentation limits its ability to propagate within a network, while strong password policies and multi-factor authentication (MFA) reduce the risk of unauthorized access [122]. Regular data backups, stored offline or in secure locations, ensure data recovery in case of infection. Employing threat intelligence feeds and monitoring for Emotet-specific indicators of compromise (IOCs) further strengthens defenses against this evolving and persistent botnet.

4.6. Colonial pipeline ransomware attack

The Colonial Pipeline ransomware attack, which occurred in May 2021, was a highly disruptive cyberattack that targeted Colonial Pipeline, one of the largest fuel pipeline operators in the United States. The attack was carried out by the DarkSide ransomware group, which used a compromised VPN account to gain access to the company's internal networks [123]. As demonstrated in Figure 8, once inside, the attackers deployed ransomware that encrypted critical data and systems, forcing Colonial Pipeline to shut down operations to contain the threat. This led to significant fuel supply disruptions along the East Coast of the U.S., causing gas shortages and price hikes [124]. The attack highlighted the vulnerability of critical infrastructure to cyber threats and underscored the growing threat of ransomware attacks on industrial systems. In response, Colonial Pipeline paid a ransom of nearly $5 million in Bitcoin, though a portion of the payment was later recovered by the U.S. authorities. The incident raised alarm over the need for enhanced cybersecurity measures within critical infrastructure sectors.

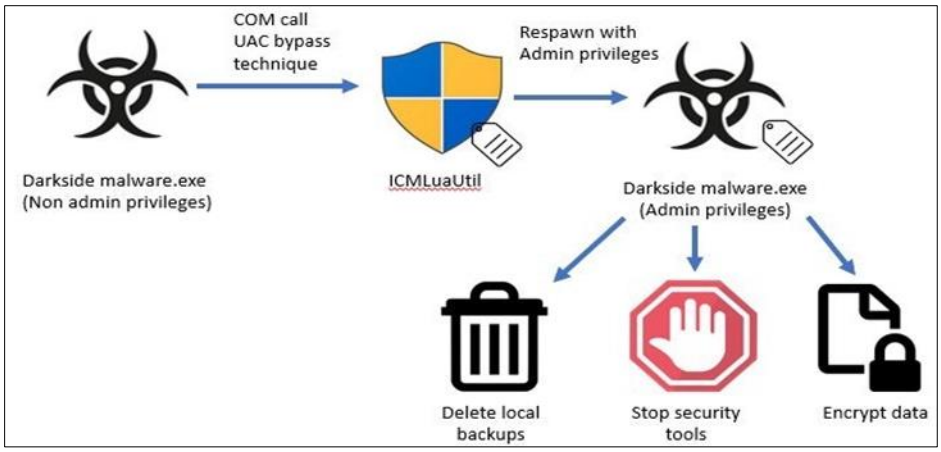

Figure 8 DarkSide ransomware

- *Impact:* The attack led to a temporary shutdown of the pipeline, causing fuel shortages and panic buying across multiple states. The company paid a ransom of $4.4 million to regain access to its systems.
- *Prevention*: Preventing DarkSide ransomware involves a comprehensive cybersecurity strategy that addresses vulnerabilities and minimizes attack surfaces [125]. Organizations should prioritize patching operating systems and software to eliminate known exploits that ransomware groups often leverage. Network segmentation is crucial to limit lateral movement and contain potential infections. Implementing strong password policies, multi-factor authentication (MFA), and privileged access management reduces the risk of compromised credentials [126], [127]. Endpoint detection and response (EDR) solutions can identify DarkSide's malicious activities, such as data exfiltration and encryption processes, in real-time. Regular backups of critical data, stored offline or in secure, immutable environments, ensure recovery without paying ransoms. Additionally, educating employees about phishing scams and social engineering tactics minimizes the chances of initial infection. Employing intrusion detection and prevention systems (IDS/IPS) and monitoring for indicators of compromise (IOCs) specific to DarkSide can help detect early stages of an attack [128]. A strong incident response plan is also essential to mitigate damage in case of compromise.

4.7. TrickBot botnet

TrickBot is a highly sophisticated and modular botnet that was first identified in 2016, initially designed as a banking Trojan to steal financial information. Over time, TrickBot evolved into a multi-purpose malware platform used to distribute additional malicious payloads, including ransomware, such as Ryuk and Conti, as well as information-stealing malware [129]. As shown in Figure 9, TrickBot spreads primarily through phishing emails, often containing malicious attachments or links to compromised websites, and can infect both individuals and organizations. Once inside a network, it uses lateral movement techniques, including credential theft and exploitation of known vulnerabilities, to propagate and maintain persistence [130]. TrickBot's modular structure allows cybercriminals to easily adapt and customize the botnet for different objectives, including data theft, espionage, and ransomware deployment. It has been a key tool for various cybercriminal groups, and despite efforts to disrupt its operations, TrickBot remains a significant threat, constantly evolving and adapting to cybersecurity defenses..

- *Impact:* Hospitals and clinics faced delays in patient care as systems were locked or data was stolen. TrickBot's ability to target financial institutions also posed a risk to the stability of financial systems.

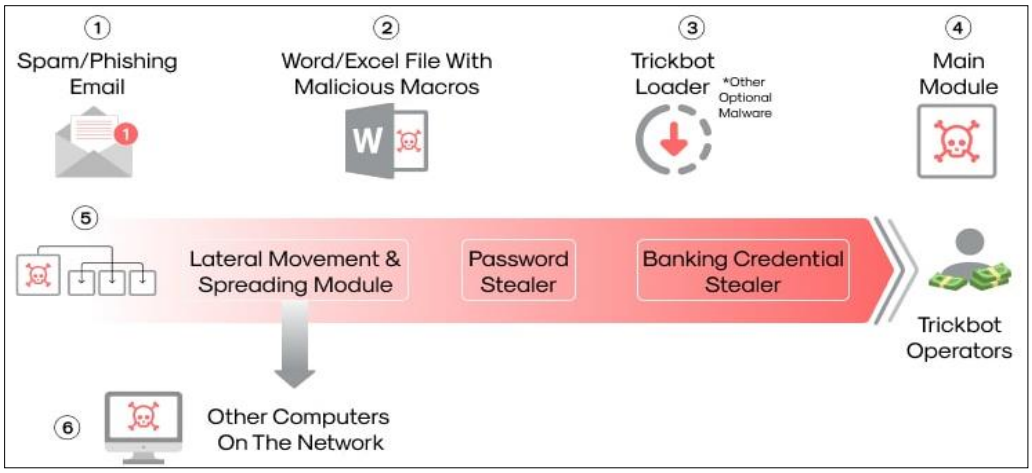

Figure 9 TrickBot Botnet

- *Prevention*: Preventing the TrickBot botnet requires a proactive and layered approach to cybersecurity, targeting both its infiltration and propagation methods. Since TrickBot commonly spreads through phishing emails, organizations should deploy advanced email filtering systems and conduct regular employee training on identifying phishing attempts [131]. Keeping all software, operating systems, and applications updated with the latest security patches is critical to addressing vulnerabilities that TrickBot exploits. Advanced endpoint protection and behavior-based detection tools can identify and block TrickBot's malicious activities, such as credential harvesting and lateral movement. Network segmentation is essential to limit the spread of the botnet within an organization, while strong password policies and MFA reduce the risk of unauthorized access [132], [133]. Regular vulnerability assessments and monitoring for TrickBot-specific indicators of compromise (IOCs) enable early detection and mitigation. Maintaining secure, offline backups of critical data further ensures recovery and minimizes damage if an infection occurs. A well-prepared incident response plan is also vital to effectively manage and contain any TrickBot-related incidents.

4.8. Mariposa botnet

The Mariposa botnet, discovered in 2008, was a large and sophisticated network of infected computers used for cybercrime activities, primarily focused on stealing personal information, distributing spam, and launching DDoS attacks [134]. It was propagated through the use of malicious email attachments and exploited vulnerabilities in software to gain control over computers, turning them into "zombies" under the control of its operators. At its peak, the Mariposa botnet had infected over 13 million computers worldwide, making it one of the largest botnets of its time [135]. As demonstrated in Figure 10, the botnet was managed through a centralized command-and-control (C&C) infrastructure, and its operators used it to conduct various illegal activities, including stealing banking credentials and executing large-scale spam campaigns. In 2010, the botnet was dismantled following an international law enforcement effort, but its impact underscored the vulnerabilities in personal computing and the growing threat of botnets for financial and cybercriminal purposes.

- *Impact:* on Critical Infrastructure: The botnet disrupted banking operations, stealing financial credentials and launching attacks on telecom companies, leading to service outages.
- *Prevention*: Preventing the Mariposa botnet, which exploits vulnerabilities in systems to create a network of infected devices, requires robust security practices focused on both system and user protection. Organizations and individuals should keep all software, operating systems, and applications updated with the latest patches to close vulnerabilities that the botnet could exploit. Employing strong antivirus and anti-malware solutions can help detect and block malicious payloads associated with Mariposa [136]. Since the botnet often spreads through phishing and social engineering tactics, educating users about recognizing suspicious emails, links, and attachments is critical. Implementing strong password policies and enabling MFA reduces the risk of unauthorized access.

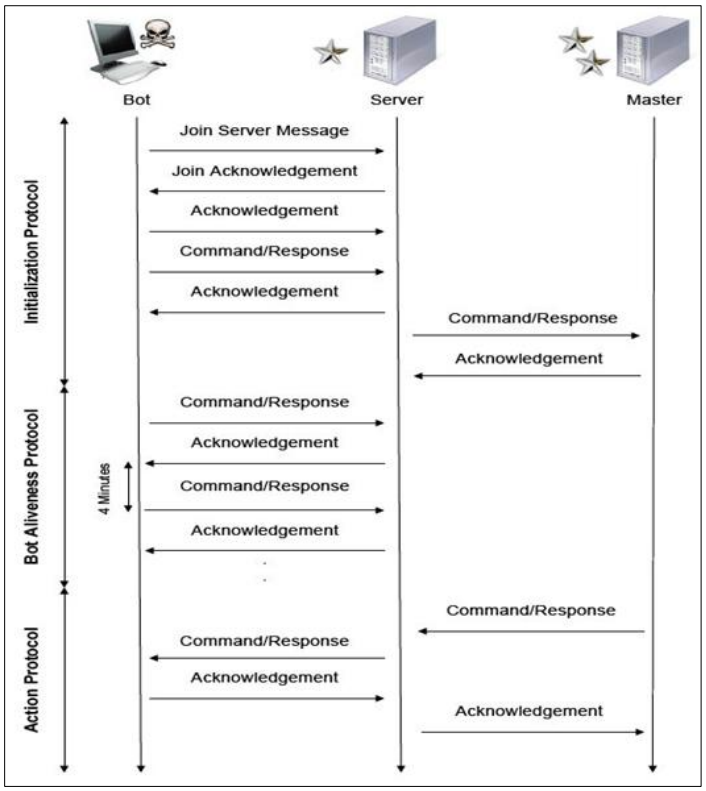

Figure 10 Mariposa botnet

Network monitoring tools can detect unusual traffic patterns that may indicate botnet activity, while firewalls and intrusion detection/prevention systems (IDS/IPS) can block malicious communication [137] with command-and-control (C&C) servers. Regular data backups and security audits further enhance resilience, ensuring systems remain protected against botnet threats like Mariposa [138]. Table 1 describes some notable examples of botnet attacks that have had significant impacts on critical infrastructure.

Table 1 Notable Botnets

Botnet	**Year**	**Sector affected**
Mirai	2016	Internet Service Providers (ISPs) Domain Name System (DNS) Infrastructure
BlackEnergy	2015	Energy
WannaCry	2017	Healthcare Transportation Finance
IoTroop Botnet	2017	IoT Infrastructure: Energy Transportation Communication
Emotet	2020	Government Healthcare Financial services
DarkSide	2021	Energy
TrickBot	2020	Healthcare

		Financial services Local governments
Mariposa	2008–2010	Telecommunications Financial services

These notable botnet attacks illustrate the diverse ways in which botnets can disrupt critical infrastructure, from causing operational outages to compromising sensitive data. They highlight the need for robust security measures, including network segmentation, timely patching, IoT security, and advanced threat detection [139], [140]. As botnets continue to evolve in scale and sophistication, addressing their threat to critical infrastructure will require collaboration among governments, private sector entities, and cybersecurity professionals.

5. Botnets and critical infrastructure performance

Botnets have emerged as one of the most pervasive threats to the stability and functionality of critical infrastructure [141]. These networks of compromised devices, controlled remotely by malicious actors, can launch large-scale and sophisticated cyberattacks that disrupt the performance of vital systems, degrade service quality, and compromise the safety and security of essential operations [142]. Critical infrastructure sectors such as energy, healthcare, transportation, water management, and financial services depend on reliable and efficient systems to deliver services to the public. Botnets, with their ability to exploit vulnerabilities and scale attacks across interconnected systems, can severely impair the performance of these infrastructures [143], [144]. Below is an extensive discussion of the specific ways in which botnets affect the performance of critical infrastructure.

5.1. Service disruptions through DDoS attacks

Botnets are frequently used to launch DDoS attacks, where a massive volume of traffic is directed at a target system to overwhelm its resources and make it unavailable to legitimate users [145]. For critical infrastructure, such disruptions can have severe consequences.

- *Energy sector*: A DDoS attack on the communication networks of a power grid can disrupt the ability to monitor and control electricity distribution [146], leading to blackouts and cascading failures in dependent sectors like healthcare and transportation.
- *Healthcare*: Hospitals and emergency response systems rely on uninterrupted internet connectivity for electronic health records, telemedicine, and operational efficiency [147]. A botnet-driven DDoS attack can delay life-saving treatments and compromise patient care.
- *Transportation*: In smart transportation systems, such as traffic management or automated rail networks, a DDoS attack can disrupt operations [148], leading to delays, accidents, and economic losses.

These service interruptions not only hinder performance but can also create public safety risks and erode trust in critical infrastructure systems.

5.2. Latency and degradation of system performance

Botnets can affect critical infrastructure performance by introducing latency and resource exhaustion [149], even in scenarios where systems are not completely taken offline.

- *Network overload*: Botnets can consume significant bandwidth and computational resources, causing delays in data processing, monitoring, and communication [150], [151]. For example, a botnet infecting smart grid IoT devices may reduce the responsiveness of load-balancing systems, affecting energy distribution efficiency.
- *Resource starvation*: Systems under botnet attack may allocate excessive resources [152] to handling malicious traffic or processes, slowing down legitimate operations. This is particularly problematic in real-time systems like air traffic control or SCADA (Supervisory Control and Data Acquisition) systems, where delays can have catastrophic consequences.

Such performance degradation can lead to reduced operational capacity, missed deadlines, and compromised service delivery across critical sectors.

5.3. Loss of system reliability and availability

Critical infrastructure systems are designed to operate with high reliability and availability [153], often following strict service-level agreements (SLAs). Botnets can undermine these goals by causing unexpected outages or performance fluctuations.

- *Energy reliability*: A botnet attack targeting energy management systems may cause irregularities in electricity distribution [154], resulting in frequent power fluctuations or outages that impact industrial and residential users.
- *Healthcare availability*: A botnet targeting healthcare systems can render medical devices or patient databases unavailable, forcing delays in diagnostics and treatment [154]-[157]. For instance, ransomware attacks enabled by botnets can lock healthcare providers out of critical systems.
- *Financial systems*: Financial services rely on high availability to process transactions and manage markets. A botnet-induced disruption can freeze trading platforms, delay payments, and lead to widespread economic instability [158], [159].

The loss of reliability and availability undermines the trust of stakeholders and the public, which is critical for the smooth functioning of infrastructure.

5.4. Impact on monitoring and control systems

Monitoring and control systems, such as SCADA and ICS, are essential for the real-time management of critical infrastructure [160], [161]. Botnets targeting these systems can impair their performance by compromising data integrity, introducing false signals, or causing delays in response actions.

- *False readings*: Botnets can manipulate data transmitted between sensors and control systems [162], providing operators with inaccurate information. For example, a water treatment facility might be misled into adjusting chemical levels incorrectly, compromising water quality [163].
- *Command execution delays*: In industrial processes, timely execution of commands is essential to maintaining operational efficiency [164], [165]. Botnet-induced delays can disrupt production schedules, damage equipment, or even cause safety hazards.
- *Loss of visibility*: By disabling monitoring tools or overloading them with false alerts, botnets can create blind spots for operators [166], reducing their ability to detect and respond to system anomalies.

These disruptions in monitoring and control can lead to inefficient operations, increased maintenance costs, and potential safety risks.

5.5. Propagation of malware and system instability

Botnets are often used to propagate malware across networks, leading to widespread system instability and performance issues [167], [168]. Malware infections can compromise device functionality, alter configurations, and create vulnerabilities for further exploitation.

- *Energy systems*: Malware introduced via botnets can disable or degrade the performance of critical components such as transformers, turbines, or communication links, reducing the overall efficiency of energy production and distribution [169], [170].
- *Transportation networks*: Malware infections in automated transportation systems can disrupt schedules, alter navigation systems, or disable critical safety features [171], [172]. For instance, a botnet attacking an automated rail network could cause scheduling conflicts and delays.
- *Healthcare devices*: Medical devices infected by malware may fail to operate correctly [173], leading to errors in diagnostics, treatment delivery, or patient monitoring.

System instability caused by malware infections can also lead to long-term performance degradation, requiring costly repairs and recovery efforts.

5.6. Economic and productivity losses

Performance degradation in critical infrastructure directly translates into economic losses and reduced productivity.

- *Operational downtime*: Delays and outages caused by botnet attacks can disrupt industrial production lines, transportation services, and public utilities, resulting in significant economic losses [174], [175].
- *Increased costs*: Infrastructure operators often need to allocate additional resources for system recovery, security upgrades, and compliance with regulatory requirements following a botnet attack [176].
- *Supply chain disruptions*: Botnet-induced performance issues in transportation and logistics systems can cause delays in supply chain operations [177], impacting industries dependent on just-in-time deliveries.

The ripple effect of these economic losses can impact local and national economies, particularly when critical industries are affected.

5.7. Cascading performance failures across interdependent systems

Modern critical infrastructure systems are highly interconnected, meaning performance issues [178] in one sector can cascade into others. For instance, an attack on the power grid can disrupt water treatment facilities that rely on electricity for pumping and purification processes. In addition, disruptions in transportation networks can delay the delivery of critical medical supplies, affecting healthcare performance [179], [180]. Moreover, performance issues in financial systems can hinder transactions necessary for the functioning of other infrastructure sectors.

Such interdependencies amplify the impact of botnets on infrastructure performance, making recovery more complex and time-consuming.

5.8. Erosion of public confidence in services

Botnet-induced performance issues can erode public trust in the reliability of critical infrastructure. Repeated disruptions or delays in services such as electricity, transportation, or healthcare can create societal unrest and reduce confidence in government and private-sector operators [181], [182]. Public dissatisfaction can further complicate recovery efforts and damage the reputations of affected organizations.

It is clear that botnets pose a substantial threat to the performance of critical infrastructure by disrupting services, degrading system efficiency, and undermining reliability and availability. Their ability to exploit vulnerabilities [183], propagate malware, and overwhelm resources creates significant challenges for infrastructure operators and stakeholders. As botnets become more sophisticated, their impact on critical infrastructure performance will likely grow, requiring proactive and comprehensive security measures to mitigate their effects and ensure the resilience of essential systems.

6. Countermeasures for botnets

Botnets represent a significant and evolving threat to cybersecurity, capable of launching large-scale attacks such as DDoS, data theft, malware distribution, and ransomware deployment [184], [185]. Countering botnets effectively requires a multifaceted approach involving technological, procedural, and policy-based interventions. Table 2 is an extensive discussion of the key countermeasures for mitigating the threat of botnets.

Table 2 Botnets countermeasures

Countermeasure	Explanation
Device Security	Botnets often exploit vulnerabilities in devices, especially IoT devices, to recruit them into their networks [186]. Enhancing device security is a foundational countermeasure. *Patch management*: Regularly updating device firmware and software to address known vulnerabilities prevents botnets from exploiting outdated systems [187]. *Secure device configuration*: Configuring devices with secure settings, such as disabling default credentials, implementing strong passwords, and minimizing unnecessary services, reduces attack surfaces. *Encryption*: Encrypting communications between devices protects against interception and unauthorized access [188] by botnets.

	Network Access Control (NAC): Restricting device access to networks based on predefined security policies [189] ensures that only authorized and secure devices can connect.
Network-based defenses	Networks are a critical point for detecting and mitigating botnet activity. *Intrusion Detection and Prevention Systems (IDPS)*: These systems monitor network traffic for anomalous patterns indicative of botnet activity and can block malicious traffic in real-time [190]. *Traffic filtering and rate limiting*: By implementing rate limiting and traffic filtering [191], networks can mitigate the effects of DDoS attacks launched by botnets. *DNS sinkholing*: Redirecting botnet traffic to a controlled environment (sinkhole) disrupts communication between botnets and their command-and-control (C&C) servers [192]. *Segmentation*: Network segmentation isolates infected devices, preventing botnets from propagating across the network.
Advanced threat detection	Sophisticated botnets employ obfuscation techniques to evade detection. Advanced threat detection systems can counteract these efforts. *Machine learning and AI*: AI-powered systems analyze vast amounts of data [193] to identify subtle patterns of botnet activity, even in encrypted traffic. *Behavioral analysis*: Analyzing device behavior to detect deviations from normal patterns can reveal botnet infections [194]. *Honeypots and honeynets*: Deploying decoy systems (honeypots) to attract and analyze botnets [195] provides valuable intelligence about their methods and targets. *Threat intelligence sharing*: Organizations can leverage shared threat intelligence to stay informed about emerging botnets and their tactics.
Mitigating C&C communications	Botnets rely on C&C servers to coordinate their activities. Disrupting this communication can neutralize their effectiveness. *Domain Generation Algorithm (DGA) monitoring*: Many botnets use DGAs to generate dynamic C&C domains [196]. Monitoring and preemptively blocking these domains can disrupt botnet operations. *IP blacklisting*: Identifying and blocking IP addresses associated with C&C servers can sever botnet communication. *Protocol analysis*: Deep packet inspection (DPI) can identify and block specific protocols used by botnets for communication [197].
Mitigating IoT-specific threats	IoT devices are a primary target for botnet recruitment due to their weak security measures. *IoT device authentication*: Implementing strong, device-specific authentication mechanisms prevents unauthorized access [198]. *Firmware integrity checks*: Regularly verifying the integrity of IoT firmware ensures that devices have not been compromised. *Device monitoring and management*: Centralized platforms for monitoring and managing IoT devices help identify and isolate infected devices [199].
Incident response and recovery	Effective response mechanisms are essential for limiting damage and recovering from botnet attacks. *Botnet infection identification*: Rapidly identifying infected devices allows organizations to isolate and remediate them.

	quarantine mechanisms: Segregating infected devices from the network prevents further spread and mitigates damage. *Backup and recovery plans*: Regularly backing up data ensures that systems can be restored quickly in the event of a ransomware attack facilitated by a botnet. *Post-attack forensics*: Analyzing botnet activity during and after an attack provides insights into vulnerabilities [200] and informs future defenses.
Collaboration with Internet Service Providers (ISPs)	ISPs are key stakeholders in botnet mitigation due to their central role in internet traffic. *Traffic analysis*: ISPs can monitor traffic for signs of botnet activity [201], such as abnormal spikes in traffic volume. *Subscriber notifications*: ISPs can notify customers when their devices are detected as part of a botnet, encouraging them to take remedial action. *Botnet takedowns*: Working with cybersecurity organizations and law enforcement, ISPs can assist in dismantling botnets by disabling their infrastructure.
Cybersecurity best practices for organizations	Organizations can adopt best practices to defend against botnets. *Zero trust architecture*: Adopting a zero-trust model [202] ensures that all devices and users are verified before granting access to critical resources. *Vulnerability management*: Regularly scanning for and addressing vulnerabilities [203] in systems and devices reduces attack surfaces. *Security awareness training*: Educating employees about phishing attacks and safe practices reduces the risk of botnet infections originating from human error. *Incident response planning*: Developing and regularly updating incident response plans ensures a coordinated and effective reaction to botnet attacks.
Proactive measures against emerging threats	As botnets evolve, proactive measures are necessary to stay ahead of new threats. *Botnet simulation and testing*: Conducting simulations of botnet attacks [204] helps organizations test their defenses and improve their readiness. *Investment in R&D*: Research and development of new detection and mitigation technologies keep defenses up-to-date with emerging botnet techniques.

Evidently, countering botnets requires a multi-layered strategy that combines technological defenses, legal and policy interventions, and public and private sector collaboration. As botnets continue to evolve, leveraging advanced detection systems, securing devices and networks, and fostering international cooperation will be critical in mitigating their impact. Organizations, governments, and individuals must work together to develop resilient defenses against this pervasive threat.

7. Research gaps future research directions

Botnets remain a critical challenge in cybersecurity, with their increasing sophistication posing a growing threat to infrastructure, businesses, and individuals [205]. Despite significant progress in detection and mitigation strategies, numerous research gaps persist. Addressing these gaps is crucial for developing robust, future-proof countermeasures against evolving botnets.

7.1. Research gaps

Research on botnets and critical infrastructure security has advanced significantly, yet several critical gaps remain, as described in Table 3. One major gap is the lack of comprehensive detection and mitigation frameworks that can adapt to the evolving sophistication of botnets, such as those employing decentralized architectures or AI-driven evasion techniques. Additionally, securing resource-constrained IoT devices, which are commonly targeted by botnets, remains a challenge due to their limited processing power and memory, which make traditional security solutions impractical.

Table 3 Research gaps

Concept	Illustration	Gap (s)	Repercussions
Gaps	Insufficient understanding of emerging botnet architectures	Botnets are adopting decentralized architectures, such as peer-to-peer (P2P) systems, making detection and mitigation challenging [206], [207]. Existing research often focuses on traditional centralized command-and-control (C&C) models, leaving decentralized systems less understood.	These decentralized botnets are more resilient to takedown attempts and can dynamically adapt to changing network conditions, which current tools and strategies struggle to counteract.
	Limited IoT-specific security solutions	The rapid proliferation of Internet of Things (IoT) devices has created new vulnerabilities [208], [209]. IoT devices are often designed with minimal security features, yet many studies neglect the unique challenges these devices present, such as constrained computational and energy resources.	Botnets like Mirai have demonstrated the catastrophic impact of IoT-based attacks. Current research lacks scalable, lightweight solutions tailored to secure IoT devices without compromising their performance.
	Inadequate real-time detection capabilities	While machine learning (ML) and artificial intelligence (AI) have been explored for botnet detection [210], many models are computationally intensive and not optimized for real-time deployment in large-scale networks.	Delays in detecting botnet activity allow malicious actors to execute attacks and spread infections, increasing the scope of damage.
	Insufficient collaboration and data sharing	Cybersecurity organizations, governments, and ISPs often work in silos, and data sharing on botnet activities is limited due to privacy concerns and the lack of standardized frameworks.	This lack of collaboration hinders comprehensive threat analysis and prevents the development of holistic countermeasures.
	Poor adaptability to evasive techniques	Botnets are increasingly employing evasion techniques such as encryption, polymorphism, and fast-flux DNS to avoid detection [211], [212]. Current detection methods often rely on static signatures or fixed behavioral patterns, which are easily bypassed.	These techniques render many traditional botnet detection and mitigation strategies obsolete, necessitating more adaptive and dynamic approaches.
	Insufficient focus on post-attack recovery	Research predominantly focuses on prevention and detection, with limited attention given to post-attack recovery strategies for systems compromised by botnets.	A lack of recovery protocols increases downtime, raises costs, and leaves systems vulnerable to reinfection.
	Lack of global regulatory frameworks	The global nature of botnets complicates enforcement and response, as botnet operators often exploit jurisdictional loopholes. Current research does not adequately address the development of enforceable international policies.	Without coordinated global efforts, botnets remain difficult to dismantle and prosecute.

Another gap lies in real-time threat intelligence sharing and coordination across nations and industries, as current efforts are often fragmented and hampered by legal and privacy concerns. The integration of artificial intelligence and machine learning [213] for predictive analysis in identifying potential botnet threats is still underexplored, particularly in critical infrastructure environments with legacy systems. Furthermore, there is limited research on quantifying the economic and operational impacts of botnet attacks on critical infrastructure, which is essential for prioritizing defense

strategies. Addressing these gaps requires interdisciplinary research, international collaboration, and the development of innovative, scalable security solutions tailored to the unique needs of critical infrastructure.

7.2. Future research directions

Future research in botnet and critical infrastructure security should focus on developing advanced detection and mitigation strategies that leverage artificial intelligence (AI) and machine learning (ML) for real-time threat identification and response. Some of these research scopes are illustrated in Table 4. With the increasing integration of IoT devices in critical infrastructure, research should explore lightweight security protocols that can operate efficiently on resource-constrained devices.

Table 4 Future research scopes

Scope	Focus domain
Resilient detection mechanisms	Employing AI and ML models [214] optimized for low-latency, real-time botnet detection. Investigating hybrid detection systems that combine signature-based, anomaly-based, and behavior-based methods [215] for comprehensive coverage. Developing unsupervised learning techniques for detecting previously unknown botnet patterns [216] without relying on labeled datasets.
Advancing IoT security solutions	Designing lightweight cryptographic protocols that enhance IoT security without straining device resources [217]-[219]. Exploring blockchain-based security frameworks [220] for authenticating and verifying IoT device interactions. Creating unified IoT device security standards and protocols to minimize vulnerabilities across different manufacturers and platforms [221]-[224].
Decentralized botnet countermeasures	Researching methods to disrupt peer-to-peer communication in decentralized botnets [225]. Exploring network topology analysis to identify and isolate nodes within decentralized botnets [226]. Developing strategies to track and sinkhole botnet traffic [227] in decentralized environments.
Collaboration and threat intelligence sharing	Establishing standardized frameworks for secure, anonymized sharing of botnet-related data among stakeholders [228], [229]. Promoting international collaboration to facilitate joint botnet takedowns and cross-border enforcement actions. Integrating federated learning models to enable organizations to train botnet detection systems [230] on shared data without compromising privacy.
Countering evasion techniques	Employing adversarial machine learning to anticipate and counter botnet evasion strategies [231], [232]. Investigating deep packet inspection (DPI) and encrypted traffic analysis [233] for detecting botnets using encrypted communications. Developing tools to identify and mitigate fast-flux DNS [234] and other dynamic C&C techniques.
Post-attack recovery	Researching automated recovery frameworks that enable systems to self-heal after botnet-induced disruptions. Developing backup strategies and data integrity verification tools [235] to ensure rapid restoration of services. Establishing guidelines for system reconfiguration and hardening to prevent reinfection.

Proactive measures	Conducting botnet simulation studies to predict future botnet architectures and attack vectors. Integrating threat modeling and risk assessment tools [236] into the design phase of critical infrastructure projects. Promoting honeynet deployments to gather intelligence on botnet behavior and vulnerabilities.

There is also significant scope for creating decentralized and blockchain-based frameworks for resilient command-and-control disruption, reducing the effectiveness of botnets [237]. Enhancing predictive analytics to identify emerging threats and vulnerabilities before exploitation is another vital area. Interdisciplinary studies that combine cybersecurity with risk management, policy development, and economic impact analysis are needed to inform robust defenses and allocate resources effectively. Additionally, fostering international collaboration on threat intelligence sharing [238] and establishing unified standards for securing critical infrastructure can play a transformative role in mitigating botnet risks globally. Addressing these areas will be critical for building resilient systems capable of withstanding the evolving botnet threat landscape.

8. Conclusion

Botnets represent one of the most persistent and disruptive threats to the security of critical infrastructure across multiple sectors, including energy, healthcare, finance, and telecommunications. As the scale and sophistication of botnet attacks continue to evolve, the implications for critical infrastructure security have grown significantly. This paper has explored the architecture, methods of attack, and impact of botnets on critical infrastructure, highlighting both the vulnerabilities and the challenges they pose. The key takeaway from this survey is that while considerable progress has been made in developing countermeasures against botnets, significant gaps remain in securing critical infrastructure. The integration of new technologies like IoT, the growing use of machine learning for botnet detection, and the shift toward decentralized botnet models complicate traditional defense mechanisms. Furthermore, the lack of cohesive international policies and standards for cybersecurity in critical sectors further exacerbates the problem. In order to strengthen the security of critical infrastructure against botnets, future research must focus on improving real-time detection systems, developing lightweight security solutions for resource-constrained devices, and enhancing international collaboration for information sharing and coordinated defense. Additionally, proactive measures, such as better patch management, improved IoT security, and robust response protocols, should be incorporated into cybersecurity frameworks to limit the spread and impact of botnet infections. Ultimately, securing critical infrastructure from botnet attacks requires a multi-layered approach, encompassing technological, organizational, and policy-driven strategies. As botnets continue to evolve, it is essential for researchers, practitioners, and policymakers to stay ahead of emerging threats and continuously refine the tools and methods used to protect the backbone of modern society's infrastructure.

References

[1] Daniel SA, Victor SS. Emerging Trends in Cybersecurity for Critical Infrastructure Protection: A Comprehensive Review. Computer Science & IT Research Journal. 2024 Mar 10;5(3):576-93.

[2] Radvanovsky R, McDougall A. Critical infrastructure: homeland security and emergency preparedness. crc press; 2023 Dec 6.

[3] Daousis S, Peladarinos N, Cheimaras V, Papageorgas P, Piromalis DD, Munteanu RA. Overview of Protocols and Standards for Wireless Sensor Networks in Critical Infrastructures. Future Internet. 2024 Jan 21;16(1):33.

[4] George AS, Baskar T, Srikaanth PB. Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. Partners Universal International Innovation Journal. 2024 Feb 25;2(1):51-75.

[5] Vegesna VV. Cybersecurity of Critical Infrastructure. International Machine learning journal and Computer Engineering. 2024 Mar 14;7(7):1-7.

[6] Jawad M, Yassin AA, Al-Asadi HA, Abduljabbar ZA, Nyangaresi VO. IoHT System Authentication Through the Blockchain Technology: A Review. In2024 10th International Conference on Control, Decision and Information Technologies (CoDIT) 2024 Jul 1 (pp. 2253-2258). IEEE.

[7] Tsantikidou K, Sklavos N. Threats, Attacks, and cryptography frameworks of cybersecurity in critical infrastructures. Cryptography. 2024 Feb 25;8(1):7.

[8] Yigit Y, Ferrag MA, Sarker IH, Maglaras LA, Chrysoulas C, Moradpoor N, Janicke H. Critical infrastructure protection: Generative ai, challenges, and opportunities. arXiv preprint arXiv:2405.04874. 2024 May 8.

[9] Al-Mhdawi MK, O'connor A, Qazi A, Rahimian F, Dacre N. Review of studies on risk factors in critical infrastructure projects from 2011 to 2023. Smart and Sustainable Built Environment. 2024 Feb 16.

[10] Franken J, Reuter C. Secure Critical Infrastructures. InInformation Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace 2024 Nov 1 (pp. 279-301). Wiesbaden: Springer Fachmedien Wiesbaden.

[11] Nyangaresi VO, Alsolami E, Ahmad M. Trust-enabled Energy Efficient Protocol for Secure Remote Sensing in Supply Chain Management. IEEE Access. 2024 Aug 12.

[12] Hossain MI, Hasan R. Smart Cities: Cybersecurity Concerns. InComputer and Information Security Handbook 2025 Jan 1 (pp. 1397-1412). Morgan Kaufmann.

[13] Praditya E, Maarif S, Ali Y, Saragih HJ, Duarte R, Suprapto FA, Nugroho R. National Cybersecurity Policy Analysis for Effective Decision-Making in the Age of Artificial Intelligence. Journal of Human Security. 2023 Dec 24;19(2):91-106.

[14] Asghar MR, Hu Q, Zeadally S. Cybersecurity in industrial control systems: Issues, technologies, and challenges. Computer Networks. 2019 Dec 24;165:106946.

[15] Yadav G, Paul K. Architecture and security of SCADA systems: A review. International Journal of Critical Infrastructure Protection. 2021 Sep 1;34:100433.

[16] Radhi BM, Hussain MA, Abduljabbar ZA, Nyangaresi VO. Secure and Fast Remote Application–Based Authentication Dragonfly Using an LED Algorithm in Smart Buildings. In2024 International Conference on Artificial Intelligence in Information and Communication (ICAIIC) 2024 Feb 19 (pp. 509-517). IEEE.

[17] Li Q, Huang H, Li R, Lv J, Yuan Z, Ma L, Han Y, Jiang Y. A comprehensive survey on DDoS defense systems: New trends and challenges. Computer Networks. 2023 Jun 24:109895.

[18] El Fawal AH, Mansour A, Ammad Uddin M, Nasser A. Securing IoT Networks from DDoS Attacks Using a Temporary Dynamic IP Strategy. Sensors. 2024 Jul 1;24(13):4287.

[19] Heckel KM, Weller A. Countering Autonomous Cyber Threats. arXiv preprint arXiv:2410.18312. 2024 Oct 23.

[20] Alsheikh M, Konieczny L, Prater M, Smith G, Uludag S. The state of IoT security: Unequivocal appeal to cybercriminals, onerous to defenders. IEEE Consumer Electronics Magazine. 2021 May 14;11(3):59-68.

[21] Nyangaresi VO, El-Omari NK, Nyakina JN. Efficient Feature Selection and ML Algorithm for Accurate Diagnostics. Journal of Computer Science Research. 2022 Jan 25;4(1):10-9.

[22] Andrew L. The vulnerability of vital systems: how'critical infrastructure'became a security problem. InSecuring'the Homeland' 2020 Apr 28 (pp. 17-39). Routledge.

[23] Jensen ET. Computer attacks on critical national infrastructure: A use of force invoking the right of self-defense. Stan. J. Int'l L.. 2002;38:207.

[24] Asadi M, Jamali MA, Heidari A, Navimipour NJ. Botnets Unveiled: A Comprehensive Survey on Evolving Threats and Defense Strategies. Transactions on Emerging Telecommunications Technologies. 2024 Nov;35(11):e5056.

[25] Muhammad R, Ismail SA, Hassan NH. Botnet Detection and Incident Response in Security Operation Center (SOC): A Proposed Framework. International Journal of Advanced Computer Science & Applications. 2024 Mar 1;15(3).

[26] Alzaidi ZS, Yassin AA, Abduljabbar ZA, Nyangaresi VO. Development Anonymous Authentication Maria et al.'s Scheme of VANETs Using Blockchain and Fog Computing with QR Code Technique. In2024 10th International Conference on Control, Decision and Information Technologies (CoDIT) 2024 Jul 1 (pp. 2247-2252). IEEE.

[27] Vormayr G, Zseby T, Fabini J. Botnet communication patterns. IEEE Communications Surveys & Tutorials. 2017 Sep 6;19(4):2768-96.

[28] Taher F, Abdel-Salam M, Elhoseny M, El-Hasnony IM. Reliable machine learning model for IIoT botnet detection. IEEE Access. 2023 Mar 6;11:49319-36.

[29] Al lelah T, Theodorakopoulos G, Reinecke P, Javed A, Anthi E. Abuse of cloud-based and public legitimate services as command-and-control (C&C) infrastructure: a systematic literature review. Journal of Cybersecurity and Privacy. 2023 Sep 1;3(3):558-90.

[30] Hasan Kabla AH, Anbar M, Manickam S, Abdulrahman Alwan AA, Karuppayah S. Monitoring Peer-to-Peer Botnets: Requirements, Challenges, and Future Works. Computers, Materials & Continua. 2023 May 1;75(2).

[31] Nyangaresi VO, Al-Joboury IM, Al-sharhanee KA, Najim AH, Abbas AH, Hariz HM. A Biometric and Physically Unclonable Function-Based Authentication Protocol for Payload Exchanges in Internet of Drones. e-Prime-Advances in Electrical Engineering, Electronics and Energy. 2024 Feb 23:100471.

[32] Abdelkader S, Amissah J, Kinga S, Mugerwa G, Emmanuel E, Mansour DE, Bajaj M, Blazek V, Prokop L. Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks. Results in Engineering. 2024 Jul 30:102647.

[33] Sousa B, Dias D, Antunes N, Cámara J, Wagner R, Schmerl B, Garlan D, Fidalgo P. MONDEO-Tactics5G: Multistage botnet detection and tactics for 5G/6G networks. Computers & Security. 2024 May 1;140:103768.

[34] Haider RZ, Aslam B, Abbas H, Iqbal Z. C2-Eye: framework for detecting command and control (C2) connection of supply chain attacks. International Journal of Information Security. 2024 Apr 29:1-5.

[35] Singh NJ, Hoque N, Singh KR, Bhattacharyya DK. Botnet-based IoT network traffic analysis using deep learning. Security and Privacy. 2024 Mar;7(2):e355.

[36] Alshuraify A, Yassin AA, Abduljabbar ZA, Nyangaresi VO. Blockchain-based Authentication Scheme in Oil and Gas Industry Data with Thermal CCTV Cameras Applications to Mitigate Sybil and 51% Cyber Attacks. International Journal of Intelligent Engineering & Systems. 2024 Nov 1;17(6).

[37] Ling Y, Tang F, Li X, Bin D, Yang C. Research on intelligent botnet defense and analysis technology based on dynamic adversarial models. InThird International Conference on Algorithms, Microchips, and Network Applications (AMNA 2024) 2024 Jun 8 (Vol. 13171, pp. 547-553). SPIE.

[38] Barnett M, Womack J, Brito C, Miller K, Potter L, Palmer XL. Botnets in Healthcare: Threats, Vulnerabilities, and Mitigation Strategies. InEuropean Conference on Cyber Warfare and Security 2024 Jun 21 (Vol. 23, No. 1, pp. 58-65).

[39] Al-Fawa'reh M, Abu-Khalaf J, Szewczyk P, Kang JJ. MalBoT-DRL: Malware botnet detection using deep reinforcement learning in IoT networks. IEEE Internet of Things Journal. 2023 Oct 12.

[40] Singh S, Sharma M, Hossain SA. Navigating the Threat Landscape of IoT: An Analysis of Attacks. InInternational Conference On Innovative Computing And Communication 2024 Feb 16 (pp. 25-48). Singapore: Springer Nature Singapore.

[41] Ali AH, Jasim HM, Abduljabbar ZA, Nyangaresi VO, Umran SM, Ma J, Honi DG. Provably Efficient and Fast Technique for Determining the Size of a Brain Tumor in T1 MRI Images. In2024 International Conference on Artificial Intelligence in Information and Communication (ICAIIC) 2024 Feb 19 (pp. 608-613). IEEE.

[42] EL Yamani Y, Baddi Y, EL Kamoun N. A survey: contribution of ML & DL to the detection & prevention of botnet attacks. Journal of Reliable Intelligent Environments. 2024 Jun 24:1-8.

[43] Burns MG. Managing energy security: an all hazards approach to critical infrastructure. Routledge; 2019 Mar 29.

[44] Tekinerdogan B, Akşit M, Catal C, Alskaif T, Hurst W. Critical infrastructures: Key concepts and challenges. InManagement and Engineering of Critical Infrastructures 2024 Jan 1 (pp. 13-52). Academic Press.

[45] Riggs H, Tufail S, Parvez I, Tariq M, Khan MA, Amir A, Vuda KV, Sarwat AI. Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. Sensors. 2023 Apr 17;23(8):4060.

[46] Nyangaresi VO. Extended Chebyshev Chaotic Map Based Message Verification Protocol for Wireless Surveillance Systems. InComputer Vision and Robotics: Proceedings of CVR 2022 2023 Apr 28 (pp. 503-516). Singapore: Springer Nature Singapore.

[47] Mallick MA, Nath R. Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. World Scientific News. 2024;190(1):1-69.

[48] Agnew D, Boamah S, Bretas A, McNair J. Network Security Challenges and Countermeasures for Software-Defined Smart Grids: A Survey. Smart Cities. 2024 Aug 2;7(4):2131-81.

[49] Uddin R, Kumar SA, Chamola V. Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions. Ad Hoc Networks. 2024 Jan 1;152:103322.

[50] Kumari P, Jain AK. A comprehensive study of DDoS attacks over IoT network and their countermeasures. Computers & Security. 2023 Apr 1;127:103096.

[51] Nyangaresi VO, Moundounga AR. Secure data exchange scheme for smart grids. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[52] Husnoo MA, Anwar A, Chakrabortty RK, Doss R, Ryan MJ. Differential privacy for IoT-enabled critical infrastructure: A comprehensive survey. IEEE Access. 2021 Oct 29;9:153276-304.

[53] Habibzadeh H, Nussbaum BH, Anjomshoa F, Kantarci B, Soyata T. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. Sustainable Cities and Society. 2019 Oct 1;50:101660.

[54] Jimmy FN. Cybersecurity Threats and Vulnerabilities in Online Banking Systems. Valley International Journal Digital Library. 2024 Oct 1:1631-46.

[55] Despotović A, Parmaković A, Miljković M. Cybercrime and cyber security in fintech. InDigital transformation of the financial industry: approaches and applications 2023 Jan 30 (pp. 255-272). Cham: Springer International Publishing.

[56] Al Sibahee MA, Abduljabbar ZA, Ngueilbaye A, Luo C, Li J, Huang Y, Zhang J, Khan N, Nyangaresi VO, Ali AH. Blockchain-Based Authentication Schemes in Smart Environments: A Systematic Literature Review. IEEE Internet of Things Journal. 2024 Jul 3.

[57] Honnavalli B P, Sushma E, Rao A, Girimaji V, Girimaji V, Katta A. Comparative Analysis of Botnet and Ransomware for Early Detection. InInternational Conference on Next Generation Wired/Wireless Networking 2023 Dec 21 (pp. 296-308). Cham: Springer Nature Switzerland.

[58] Al-Hawawreh M, Alazab M, Ferrag MA, Hossain MS. Securing the Industrial Internet of Things against ransomware attacks: A comprehensive analysis of the emerging threat landscape and detection mechanisms. Journal of Network and Computer Applications. 2023 Dec 4:103809.

[59] Bajpai P, Enbody R. Know thy ransomware response: a detailed framework for devising effective ransomware response strategies. Digital Threats: Research and Practice. 2023 Oct 20;4(4):1-9.

[60] Pestana G, Sofou S. Data Governance to Counter Hybrid Threats against Critical Infrastructures. Smart Cities. 2024 Jul 22;7(4):1857-77.

[61] Nyangaresi VO. Provably secure authentication protocol for traffic exchanges in unmanned aerial vehicles. High-Confidence Computing. 2023 Sep 15:100154.

[62] Chakravarthi MK, Kumar YP, Reddy GP. Potential Technological Advancements in the Future of Process Control and Automation. In2024 IEEE Open Conference of Electrical, Electronic and Information Sciences (eStream) 2024 Apr 25 (pp. 1-6). IEEE.

[63] Filip FG, Leiviskä K. Infrastructure and complex systems automation. InSpringer Handbook of Automation 2023 Jun 17 (pp. 617-640). Cham: Springer International Publishing.

[64] Majhi AA, Mohanty S. A Comprehensive Review on Internet of Things Applications in Power Systems. IEEE Internet of Things Journal. 2024 Aug 21.

[65] Achaal B, Adda M, Berger M, Ibrahim H, Awde A. Study of smart grid cyber-security, examining architectures, communication networks, cyber-attacks, countermeasure techniques, and challenges. Cybersecurity. 2024 May 2;7(1):10.

[66] Ali ZA, Abduljabbar ZA, AL-Asadi HA, Nyangaresi VO, Abduljaleel IQ, Aldarwish AJ. A Provably Secure Anonymous Authentication Protocol for Consumer and Service Provider Information Transmissions in Smart Grids. Cryptography. 2024 May 9;8(2):20.

[67] Lehto M. Cyber-attacks against critical infrastructure. InCyber security: Critical infrastructure protection 2022 Apr 3 (pp. 3-42). Cham: Springer International Publishing.

[68] Djenna A, Harous S, Saidouni DE. Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. Applied Sciences. 2021 May 17;11(10):4580.

[69] Stellios I, Kotzanikolaou P, Psarakis M, Alcaraz C, Lopez J. A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. IEEE Communications Surveys & Tutorials. 2018 Jul 12;20(4):3453-95.

[70] Carlo MA, Breda P. Impact of space systems capabilities and their role as critical infrastructure. International Journal of Critical Infrastructure Protection. 2024 Jul 1;45:100680.

[71] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432). IEEE.

[72] Gajjar VR, Taherdoost H. Cybercrime on a Global Scale: Trends, Policies, and Cybersecurity Strategies. In2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI) 2024 Jan 18 (pp. 668-676). IEEE.

[73] Lakhani R. Cybersecurity Threats in Internet of Things (IoT) Networks: Vulnerabilities and Defense Mechanisms. Valley International Journal Digital Library. 2023 Nov 30:25965-80.

[74] Urias V, Van Leeuwen B. Experimental methods for control system security research. Cyber-Security of SCADA and Other Industrial Control Systems. 2016:253-77.

[75] Mohanty K, Bopche GS, Sahoo KS. A Viral Decoy Environment for Ransomware Defense. InCloud of Things 2024 Aug 7 (pp. 308-330). Chapman and Hall/CRC.

[76] Bulbul SS, Abduljabbar ZA, Mohammed RJ, Al Sibahee MA, Ma J, Nyangaresi VO, Abduljaleel IQ. A provably lightweight and secure DSSE scheme, with a constant storage cost for a smart device client. Plos one. 2024 Apr 25;19(4):e0301277.

[77] Aslan Ö, Aktuğ SS, Ozkan-Okay M, Yilmaz AA, Akin E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics. 2023 Mar 11;12(6):1333.

[78] Omolara AE, Alabdulatif A, Abiodun OI, Alawida M, Alabdulatif A, Arshad H. The internet of things security: A survey encompassing unexplored areas and new insights. Computers & Security. 2022 Jan 1;112:102494.

[79] Griffioen H, Doerr C. Examining mirai's battle over the internet of things. InProceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security 2020 Oct 30 (pp. 743-756).

[80] Macaulay T. Critical Infrastructure Interdependency: Measuring a Moving Target. Pulse & Praxis: The Journal for Critical Infrastructure Protection, Security and Resilience. 2024 Mar 4.

[81] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[82] Usama M, Ullah U, Sajid A. Cyber Attacks Against Intelligent Transportation Systems. InCyber Security for Next-Generation Computing Technologies 2024 (pp. 190-230). CRC Press.

[83] Arshi O, Rai A, Gupta G, Pandey JK, Mondal S. IoT in energy: a comprehensive review of technologies, applications, and future directions. Peer-to-Peer Networking and Applications. 2024 Jun 4:1-40.

[84] Toledano SA. Critical Infrastructure Security: Cybersecurity lessons learned from real-world breaches. Packt Publishing Ltd; 2024 May 24.

[85] Das DK. Exploring the Symbiotic Relationship between Digital Transformation, Infrastructure, Service Delivery, and Governance for Smart Sustainable Cities. Smart Cities. 2024 Mar 25;7(2):806-35.

[86] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA. Low complexity smart grid security protocol based on elliptic curve cryptography, biometrics and hamming distance. Plos one. 2024 Jan 23;19(1):e0296781.

[87] Singh M, Singh M, Kaur S. Issues and challenges in DNS based botnet detection: A survey. Computers & Security. 2019 Sep 1;86:28-52.

[88] Yadav S. Social automation and APT attributions in national cybersecurity. Journal of Cyber Security Technology. 2024 Feb 7:1-26.

[89] Repetto M. Adaptive monitoring, detection, and response for agile digital service chains. Computers & Security. 2023 Sep 1;132:103343.

[90] Jimmy FN. Cyber security Vulnerabilities and Remediation Through Cloud Security Tools. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023. 2024 Apr 12;2(1):129-71.

[91] Nyangaresi VO, Morsy MA. Towards privacy preservation in internet of drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[92] Papastergiou S, Mouratidis H, Kalogeraki EM. Handling of advanced persistent threats and complex incidents in healthcare, transportation and energy ICT infrastructures. Evolving Systems. 2021 Mar;12(1):91-108.

[93] Bederna Z, Rajnai Z, Szadeczky T. Attacks against energy, water and other critical infrastructure in the EU. In2020 IEEE 3rd International Conference and Workshop in Óbuda on Electrical and Power Engineering (CANDO-EPE) 2020 Nov 18 (pp. 000125-000130). IEEE.

[94] Kumar B, Sethia R. Analysing the Effectiveness of Intrusion Detection Systems against the Mirai Botnet: A Comparative Study. Grenze International Journal of Engineering & Technology (GIJET). 2024 Jan 15;10.

[95] Goyal M, Mittal S. Review for Prevention of Botnet Attack Using Various Detection Techniques in IoT and IIoT. In2024 2nd International Conference on Disruptive Technologies (ICDT) 2024 Mar 15 (pp. 259-264). IEEE.

[96] Al Sibahee MA, Nyangaresi VO, Abduljabbar ZA, Luo C, Zhang J, Ma J. Two-Factor Privacy Preserving Protocol for Efficient Authentication in Internet of Vehicles Networks. IEEE Internet of Things Journal. 2023 Dec 7.

[97] Fukushima A, Yamamoto Y, Yamaguchi S. Implementation of Infection Environment for White-hat Worm and Malicious Botnet Using Mirai Source Code. In2024 12th International Conference on Information and Education Technology (ICIET) 2024 Mar 18 (pp. 424-428). IEEE.

[98] Dahiya P, Bhattacharya S. MiraiBotGuard: Federated Learning for Intelligent Defense Against Mirai Threats. In2024 2nd International Conference on Device Intelligence, Computing and Communication Technologies (DICCT) 2024 Mar 15 (pp. 1-6). IEEE.

[99] Korba AA, Diaf A, Ghamri-Doudane Y. AI-Driven Fast and Early Detection of IoT Botnet Threats: A Comprehensive Network Traffic Analysis Approach. In2024 International Wireless Communications and Mobile Computing (IWCMC) 2024 May 27 (pp. 1779-1784). IEEE.

[100] Divya SB, Mary SP. A comparative analysis of using Deep Learning and Machine Learning technologies for intrusion detection for effective network traffic analysis. In2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT) 2024 Aug 8 (Vol. 1, pp. 563-569). IEEE.

[101] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1;142:103117.

[102] Aljohani TM. Cyberattacks on Energy Infrastructures as Modern War Weapons—Part I: Analysis and Motives. IEEE Technology and Society Magazine. 2024 May 15.

[103] Komninos T, Serpanos D. Cyberwarfare in Ukraine: Incidents, Tools and Methods. InHybrid Threats, Cyberterrorism and Cyberwarfare 2024 (pp. 127-147). CRC Press.

[104] Stoddart K. Cyberwar: Attacking Critical Infrastructure. InCyberwarfare: Threats to Critical Infrastructure 2022 Nov 19 (pp. 147-225). Cham: Springer International Publishing.

[105] Mishchenko D, Oleinikova I, Erdődi L, Pokhrel BR. Multidomain Cyber-Physical Testbed for Power System Vulnerability Assessment. IEEE Access. 2024 Mar 11.

[106] Djenna A, Belaoued M, Lifa N. Top Cyber Threats: The Rise of Ransomware. InIFIP International Conference on Information Security Theory and Practice 2024 Feb 29 (pp. 80-95). Cham: Springer Nature Switzerland.

[107] Mohialdin SH, Abdulrahman LQ, Al-Yoonus MH, Abduljabbar ZA, Honi DG, Nyangaresi VO, Abduljaleel IQ, Neamah HA. Utilizing Machine Learning for the Early Detection of Coronary Heart Disease. Engineering, Technology & Applied Science Research. 2024 Oct 9;14(5):17363-75.

[108] Hyslip TS, Burruss GW. Ransomware. InHandbook on Crime and Technology 2023 Mar 28 (pp. 86-104). Edward Elgar Publishing.

[109] Diamantopoulos D, Pletka R, Sarafijanovic S, Reddy AN, Pozidis H. WannaLaugh: A Configurable Ransomware Emulator-Learning to Mimic Malicious Storage Traces. InProceedings of the 17th ACM International Systems and Storage Conference 2024 Sep 16 (pp. 118-131).

[110] Sheeraz M, Durad H, Tahir S, Tahir H, Saeed S, Almuhaideb AM. Advancing Snort IPS to Achieve Line Rate Traffic Processing for Effective Network Security Monitoring. IEEE Access. 2024 Apr 29.

[111] Sutheekshan B, Basheer S, Thangavel G, Sharma OP. Evolution of Malware Targeting IoT Devices and Botnet formation. In2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT) 2024 Feb 9 (Vol. 5, pp. 1415-1422). IEEE.

[112] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[113] Kulbacki M, Chaczko Z, Barton S, Wajs-Chaczko P, Nikodem J, Rozenblit JW, Klempous R, Ito A, Kulbacki M. A Review of the Weaponization of IoT: Security Threats and Countermeasures. In2024 IEEE 18th International Symposium on Applied Computational Intelligence and Informatics (SACI) 2024 May 23 (pp. 000279-000284). IEEE.

[114] Jeebodh MR, Baliyan N. IoT Malware Detection Using Deep Learning. In2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT) 2024 Jun 24 (pp. 1-6). IEEE.

[115] Huang M, Lee H, Kundu A, Chen X, Mudgerikar A, Li N, Bertino E. Ariotedef: Adversarially robust iot early defense system based on self-evolution against multi-step attacks. ACM Transactions on Internet of Things. 2024 Jun 17;5(3):1-34.

[116] Sharma R, Sharma N, Ahmed MA. Balancing Data Fluctuations in Lightweight Attack Detection Systems for IoT Networks: A Complexity Metrics Perspective. Fluctuation and Noise Letters. 2024 Jul 5.

[117] Duaa Fadhel Najem, Nagham Abdulrasool Taha, Zaid Ameen Abduljabbar, Vincent Omollo Nyangaresi, Junchao Ma and Dhafer G. Honi. Low-Complexity and Secure Clustering-Based Similarity Detection for Private Files. TEM Journal, 13(2), 2341-2349 (2024).DOI: 10.18421/TEM133-61

[118] Chung JM. Emerging Cyber-Attacks. InEmerging Secure Networks, Blockchains and Smart Contract Technologies 2024 Sep 17 (pp. 1-29). Cham: Springer Nature Switzerland.

[119] Ismail Z, Jantan A, Yusoff MN, Kiru MU. The effects of feature selection on the classification of encrypted botnet. Journal of Computer Virology and Hacking Techniques. 2021 Mar;17:61-74.

[120] Gupta S, Alexander J, Bartwal K, Narang H, Rawat D, Aeri M. Securing Cyberspace: Traditional vs. IoT Botnets-A Machine Learning Classification Approach. In2024 1st International Conference on Advanced Computing and Emerging Technologies (ACET) 2024 Aug 23 (pp. 1-6). IEEE.

[121] Bazarkina D, Kolotaev Y, Pashentsev E, Matyashova D. Current and Potential Malicious Use of Artificial Intelligence Threats in the Psychological Domain: The Case of Japan. InThe Palgrave Handbook of Malicious Use of AI and Psychological Security 2023 Jun 10 (pp. 419-451). Cham: Springer International Publishing.

[122] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. InThe Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 2022 Jun 12 (pp. 81-99). Cham: Springer International Publishing.

[123] Beerman J, Berent D, Falter Z, Bhunia S. A review of colonial pipeline ransomware attack. In2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW) 2023 May 1 (pp. 8-15). IEEE.

[124] Pitman L, Crosier W. On the scale from ransomware to cyberterrorism: the cases of JBS USA, colonial pipeline and the wiperware attacks against Ukraine. Journal of Cyber Policy. 2024 Jul 19:1-21.

[125] Goodell JW, Corbet S. Commodity market exposure to energy-firm distress: Evidence from the Colonial Pipeline ransomware attack. Finance Research Letters. 2023 Jan 1;51:103329.

[126] Christopher T. Securing the Keys to the Kingdom: A Comprehensive Guide to Privileged Access Management Tools and Strategies. Revista de Inteligencia Artificial en Medicina. 2024 May 21;15(1):939-48.

[127] Al Sibahee MA, Abduljabbar ZA, Luo C, Zhang J, Huang Y, Abduljaleel IQ, Ma J, Nyangaresi VO. Hiding scrambled text messages in speech signals using a lightweight hyperchaotic map and conditional LSB mechanism. Plos one. 2024 Jan 3;19(1):e0296469.

[128] Al-Quayed F, Ahmad Z, Humayun M. A situation based predictive approach for cybersecurity intrusion detection and prevention using machine learning and deep learning algorithms in wireless sensor networks of industry 4.0. IEEE Access. 2024 Mar 1.

[129] Abou El Houda Z. Cyber threat actors review: examining the tactics and motivations of adversaries in the cyber landscape. InCyber Security for Next-Generation Computing Technologies 2024 (pp. 84-101). CRC Press.

[130] MacColl J, Stevens T. Countering non-state actors in cyberspace. InResearch Handbook on Cyberwarfare 2024 Jul 16 (pp. 280-300). Edward Elgar Publishing.

[131] Gezer A, Warner G, Wilson C, Shrestha P. A flow-based approach for Trickbot banking trojan detection. Computers & Security. 2019 Jul 1;84:179-92.

[132] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[133] Javed R, Vashisth R, Sindhwani N. Study on cybersecurity: Trending challenges, emerging trends, and threats. Computational Intelligence in the Industry 4.0.:108-26.

[134] Everson D, Cheng L. A Survey on Network Attack Surface Mapping. Digital Threats: Research and Practice. 2024.

[135] Moorthy RS, Nathiya N. Botnet detection using artificial intelligence. Procedia Computer Science. 2023 Jan 1;218:1405-13.

[136] Georgoulias D, Pedersen JM, Falch M, Vasilomanolakis E. Botnet business models, takedown attempts, and the darkweb market: A survey. ACM Computing Surveys. 2023 Feb 9;55(11):1-39.

[137] Umran SM, Lu S, Abduljabbar ZA, Nyangaresi VO. Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry. Internet of Things. 2023 Dec 1;24:100969.

[138] Adekanmbi O, Wimmer H, Shalan A. Semantic Web Ontology for Botnet Classification. InSemantic Intelligence: Select Proceedings of ISIC 2022 2023 Apr 1 (pp. 43-54). Singapore: Springer Nature Singapore.

[139] Salayma M. Risk and threat mitigation techniques in internet of things (IoT) environments: a survey. Frontiers in The Internet of Things. 2024 Jan 23;2:1306018.

[140] Sándor B, Rajnai Z. Smart Building IoT Cybersecurity: A Review of Threats and Mitigation Technique. In2023 IEEE 21st Jubilee International Symposium on Intelligent Systems and Informatics (SISY) 2023 Sep 21 (pp. 000321-000326). IEEE.

[141] Tariq U, Ahmed I, Bashir AK, Shaukat K. A critical cybersecurity analysis and future research directions for the internet of things: a comprehensive review. Sensors. 2023 Apr 19;23(8):4117.

[142] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

[143] Jain R, Nihalani N. Botnet Detection in Distributed Network Using Machine Learning-A Detailed Review. In2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE) 2024 May 9 (pp. 888-895). IEEE.

[144] Nazir A, He J, Zhu N, Wajahat A, Ma X, Ullah F, Qureshi S, Pathan MS. Advancing IoT security: A systematic review of machine learning approaches for the detection of IoT botnets. Journal of King Saud University-Computer and Information Sciences. 2023 Nov 6:101820.

[145] Alshahrani MM. A Secure and intelligent software-defined networking framework for future smart cities to prevent DDoS Attack. Applied Sciences. 2023 Aug 30;13(17):9822.

[146] Huseinović A, Mrdović S, Bicakci K, Uludag S. A survey of denial-of-service attacks and solutions in the smart grid. IEEE Access. 2020 Sep 25;8:177447-70.

[147] Al-Chaab W, Abduljabbar ZA, Abood EW, Nyangaresi VO, Mohammed HM, Ma J. Secure and Low-Complexity Medical Image Exchange Based on Compressive Sensing and LSB Audio Steganography. Informatica. 2023 May 31;47(6).

[148] Hatzivasilis G, Fysarakis K, Ioannidis S, Hatzakis I, Vardakis G, Papadakis N, Spanoudakis G. SPD-Safe: Secure administration of railway intelligent transportation systems. Electronics. 2021 Jan 5;10(1):92.

[149] Razaque A, Yoo J, Bektemyssova G, Alshammari M, Chinibayeva TT, Amanzholova S, Alotaibi A, Umutkulov D. Efficient Internet-of-Things Cyberattack Depletion Using Blockchain-Enabled Software-Defined Networking and 6G Network Technology. Sensors. 2023 Dec 7;23(24):9690.

[150] Kumar A, Shridhar M, Swaminathan S, Lim TJ. Machine learning-based early detection of IoT botnets using network-edge traffic. Computers & Security. 2022 Jun 1;117:102693.

[151] Wei C, Xie G, Diao Z. A lightweight deep learning framework for botnet detecting at the IoT edge. Computers & Security. 2023 Jun 1;129:103195.

[152] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1;133:102763.

[153] Šarūnienė I, Martišauskas L, Krikštolaitis R, Augutis J, Setola R. Risk assessment of critical infrastructures: A methodology based on criticality of infrastructure elements. Reliability Engineering & System Safety. 2024 Mar 1;243:109797.

[154] Merlino V, Allegra D. Energy-based approach for attack detection in IoT devices: A survey. Internet of Things. 2024 Aug 2:101306.

[155] Messinis S, Temenos N, Protonotarios NE, Rallis I, Kalogeras D, Doulamis N. Enhancing Internet of Medical Things security with artificial intelligence: A comprehensive review. Computers in Biology and Medicine. 2024 Jan 28:108036.

[156] Khatun MA, Memon SF, Eising C, Dhirani LL. Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation. IEEE Access. 2023 Dec 22.

[157] Mohammed RJ, Ghrabat MJ, Abduljabbar ZA, Nyangaresi VO, Abduljaleel IQ, Ali AH, Honi DG, Neamah HA. A Robust Hybrid Machine and Deep Learning-based Model for Classification and Identification of Chest X-ray Images. Engineering, Technology & Applied Science Research. 2024 Oct 9;14(5):16212-20.

[158] Gelgi M, Guan Y, Arunachala S, Samba Siva Rao M, Dragoni N. Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques. Sensors. 2024 Jun 1;24(11):3571.

[159] Pal R, Siegel M, Sequeira RX. A Mathematical Theory to Quantify Cyber-Resilience in IT/OT Networks. InProceedings of the Winter Simulation Conference 2023 Dec 10 (pp. 624-635).

[160] Altaleb H, Zoltán R. A Comprehensive Analysis and Solutions for Enhancing SCADA Systems Security in Critical Infrastructures. In2024 IEEE 11th International Conference on Computational Cybernetics and Cyber-Medical Systems (ICCC) 2024 Apr 4 (pp. 1-6). IEEE.

[161] Aslam MM, Tufail A, Apong RA, De Silva LC, Raza MT. Scrutinizing Security in Industrial Control Systems: An Architectural Vulnerabilities and Communication Network Perspective. IEEE Access. 2024 Apr 29.

[162] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[163] Krishnan SR, Nallakaruppan MK, Chengoden R, Koppu S, Iyapparaja M, Sadhasivam J, Sethuraman S. Smart water resource management using Artificial Intelligence—A review. Sustainability. 2022 Oct 17;14(20):13384.

[164] Gogri D. Advanced and Scalable Real-Time Data Analysis Techniques for Enhancing Operational Efficiency, Fault Tolerance, and Performance Optimization in Distributed Computing Systems and Architectures. International Journal of Machine Intelligence for Smart Applications. 2023 Dec 16;13(12):46-70.

[165] Wang CN, Vo TT, Hsu HP, Chung YC, Nguyen NT, Nhieu NL. Improving processing efficiency through workflow process reengineering, simulation and value stream mapping: a case study of business process reengineering. Business Process Management Journal. 2024 Jul 17.

[166] Rahal R, Amara Korba A, Ghoualmi-Zine N, Challal Y, Ghamri-Doudane MY. AntibotV: A multilevel behaviour-based framework for botnets detection in vehicular networks. Journal of Network and Systems Management. 2022 Jan;30(1):15.

[167] Eid MM, Arunachalam R, Sorathiya V, Lavadiya S, Patel SK, Parmar J, Delwar TS, Ryu JY, Nyangaresi VO, Zaki Rashed AN. QAM receiver based on light amplifiers measured with effective role of optical coherent duobinary transmitter. Journal of Optical Communications. 2022 Jan 17(0).

[168] Acarali D, Rajarajan M, Komninos N, Zarpelão BB. Modelling the spread of botnet malware in IoT-based wireless sensor networks. Security and Communication Networks. 2019;2019(1):3745619.

[169] Tooki OO, Popoola OM. A critical review on intelligent-based techniques for detection and mitigation of cyberthreats and cascaded failures in cyber-physical power systems. Renewable Energy Focus. 2024 Sep 2:100628.

[170] Khalaf M, Ayad A, Tushar MH, Kassouf M, Kundur D. A Survey on Cyber-Physical Security of Active Distribution Networks in Smart Grids. IEEE Access. 2024 Feb 8.

[171] Al-Sabaawi A, Al-Dulaimi K, Foo E, Alazab M. Addressing malware attacks on connected and autonomous vehicles: recent techniques and challenges. Malware Analysis Using Artificial Intelligence and Deep Learning. 2021:97-119.

[172] Nyangaresi VO, Mohammad Z. Privacy preservation protocol for smart grid networks. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[173] Eliash C, Lazar I, Nissim N. SEC-CU: the security of intensive care unit medical devices and their ecosystems. IEEE Access. 2020 Mar 31;8:64193-224.

[174] Aceto G, Botta A, Marchetta P, Persico V, Pescapé A. A comprehensive survey on internet outages. Journal of Network and Computer Applications. 2018 Jul 1;113:36-63.

[175] Makrakis GM, Kolias C, Kambourakis G, Rieger C, Benjamin J. Vulnerabilities and attacks against industrial control systems and critical infrastructures. arXiv preprint arXiv:2109.03945. 2021 Sep 8.

[176] Beretas C. Information Systems Security, Detection and Recovery from Cyber Attacks. Universal Library of Engineering Technology. 2024 Aug 31;1(1).

[177] Karmous N, Aoueileyine MO, Abdelkader M, Romdhani L, Youssef N. Software-defined-networking-based one-versus-rest strategy for detecting and mitigating distributed denial-of-service attacks in smart home internet of things devices. Sensors. 2024 Aug 3;24(15):5022.

[178] Zaki Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Signal propagation parameters estimation through designed multi layer fibre with higher dominant modes using OptiFibre simulation. Journal of Optical Communications. 2022 Jun 23(0).

[179] Dasaklis TK, Tsoulfas GT. The Future of Healthcare Supply Chains: Integrating Industry 4.0 Technologies for Improved Resilience and Sustainability. InHospital Supply Chain: Challenges and Opportunities for Improving Healthcare 2024 Oct 30 (pp. 533-551). Cham: Springer Nature Switzerland.

[180] Skowron-Grabowska B, Wincewicz-Bosy M, Dymyt M, Sadowski A, Dymyt T, Wąsowska K. Healthcare supply chain reliability: the case of medical air transport. International Journal of Environmental Research and Public Health. 2022 Apr 4;19(7):4336.

[181] Skowron-Grabowska B, Wincewicz-Bosy M, Dymyt M, Sadowski A, Dymyt T, Wąsowska K. Healthcare supply chain reliability: the case of medical air transport. International Journal of Environmental Research and Public Health. 2022 Apr 4;19(7):4336.

[182] Aslam L, Khalid R, Bukhari SA, Shabbir M, Bilal ST, Aqil S. Click, Hack, Vanish: The Growing Threat of Cyberattacks on Pakistan's Financial Sectors. Harf-o-Sukhan. 2024 May 22;8(2):309-25.

[183] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Sep 1;15:100210.

[184] Koroniotis N, Moustafa N, Sitnikova E. Forensics and deep learning mechanisms for botnets in internet of things: A survey of challenges and solutions. IEEE Access. 2019 May 14;7:61764-85.

[185] Thanh Vu SN, Stege M, El-Habr PI, Bang J, Dragoni N. A survey on botnets: Incentives, evolution, detection and current trends. Future Internet. 2021 Jul 31;13(8):198.

[186] Nasir MH, Arshad J, Khan MM. Collaborative device-level botnet detection for internet of things. Computers & Security. 2023 Jun 1;129:103172.

[187] Bakhshi T, Ghita B, Kuzminykh I. A Review of IoT Firmware Vulnerabilities and Auditing Techniques. Sensors. 2024 Jan 22;24(2):708.

[188] Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA, Nyangaresi VO, Honi DG, Abdulsada AI, Jiao X. Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map. IEEE Access. 2022 Feb 11;10:26257-70.

[189] Anjum I, Kostecki D, Leba E, Sokal J, Bharambe R, Enck W, Nita-Rotaru C, Reaves B. Removing the reliance on perimeters for security using network views. InProceedings of the 27th ACM on Symposium on Access Control Models and Technologies 2022 Jun 7 (pp. 151-162).

[190] Mazhar N, Salleh R, Zeeshan M, Hameed MM, Khan N. R-IDPS: Real time SDN based IDPS system for IoT security. In2021 IEEE 18th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET) 2021 Oct 11 (pp. 71-76). IEEE.

[191] Nice MW, Gunter G, Ji J, Zhang Y, Bunting M, Barbour W, Sprinkle J, Work DB. A middle way to traffic enlightenment. In2024 ACM/IEEE 15th International Conference on Cyber-Physical Systems (ICCPS) 2024 May 13 (pp. 147-156). IEEE.

[192] Ogu EC, Ojesanmi OA, Awodele O, Kuyoro S. A botnets circumspection: The current threat landscape, and what we know so far. Information. 2019 Oct 30;10(11):337.

[193] Nyangaresi VO. Target Tracking Area Selection and Handover Security in Cellular Networks: A Machine Learning Approach. InProceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022 2023 Feb 23 (pp. 797-816). Singapore: Springer Nature Singapore.

[194] Dumitrasc V, Serral-Gracià R. User behavior analysis for malware detection. InEuropean Symposium on Research in Computer Security 2023 Sep 25 (pp. 92-110). Cham: Springer Nature Switzerland.

[195] Javadpour A, Ja'fari F, Taleb T, Shojafar M, Benzaïd C. A comprehensive survey on cyber deception techniques to improve honeypot performance. Computers & Security. 2024 Mar 1:103792.

[196] Vishvakarma DK, Bhatia A, Riha Z. Detection of algorithmically generated domain names in botnets. InAdvanced Information Networking and Applications: Proceedings of the 33rd International Conference on Advanced Information Networking and Applications (AINA-2019) 33 2020 (pp. 1279-1290). Springer International Publishing.

[197] Deri L, Fusco F. Using deep packet inspection in cybertraffic analysis. In2021 IEEE International Conference on Cyber Security and Resilience (CSR) 2021 Jul 26 (pp. 89-94). IEEE.

[198] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA. Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment. InApplied Cryptography in Computer and Communications: Second EAI International Conference, AC3 2022, Virtual Event, May 14-15, 2022, Proceedings 2022 Oct 6 (pp. 46-64). Cham: Springer Nature Switzerland.

[199] Da Xu L, Lu Y, Li L. Embedding blockchain technology into IoT for security: A survey. IEEE Internet of Things Journal. 2021 Feb 19;8(13):10452-73.

[200] Wang A, Chang W, Chen S, Mohaisen A. Delving into internet DDoS attacks by botnets: characterization and analysis. IEEE/ACM Transactions on Networking. 2018 Nov 9;26(6):2843-55.

[201] Safaei Pour M, Nader C, Friday K, Bou-Harb E. A Comprehensive Survey of Recent Internet Measurement Techniques for Cyber Security. Computers & Security. 2023 May;128(C).

[202] Azad MA, Abdullah S, Arshad J, Lallie H, Ahmed YH. Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. Internet of Things. 2024 Oct 1;27:101227.

[203] Nyangaresi VO. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 2022 Jul 9;3(5):364.

[204] Yamin MM, Katt B. Use of cyber attack and defense agents in cyber ranges: A case study. Computers & Security. 2022 Nov 1;122:102892.

[205] Yadav S. Social botnets and the challenges of cyber situation awareness. AI and Ethics. 2024 Aug 14:1-21.

[206] Kabla AH, Thamrin AH, Anbar M, Manickam S, Karuppayah S. Peer-to-peer botnets: exploring behavioural characteristics and machine/deep learning-based detection. EURASIP Journal on Information Security. 2024 May 27;2024(1):20.

[207] Fortune DC, Mathurin SS, Kalita S. HTTP-Based Peer-to-Peer Botnet Detection Using a Machine Learning Bagging Classifier. In2024 2nd International Conference on Disruptive Technologies (ICDT) 2024 Mar 15 (pp. 353-359). IEEE.

[208] Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Khalefa MS, Honi DG. MAC-Based Symmetric Key Protocol for Secure Traffic Forwarding in Drones. InFuture Access Enablers for Ubiquitous and Intelligent Infrastructures: 6th EAI International Conference, FABULOUS 2022, Virtual Event, May 4, 2022, Proceedings 2022 Sep 18 (pp. 16-36). Cham: Springer International Publishing.

[209] Butun I, Österberg P, Song H. Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. IEEE Communications Surveys & Tutorials. 2019 Nov 13;22(1):616-44.

[210] Shinan K, Alsubhi K, Alzahrani A, Ashraf MU. Machine learning-based botnet detection in software-defined network: A systematic review. Symmetry. 2021 May 12;13(5):866.

[211] Wazzan M, Algazzawi D, Bamasaq O, Albeshri A, Cheng L. Internet of Things botnet detection approaches: Analysis and recommendations for future research. Applied Sciences. 2021 Jun 20;11(12):5713.

[212] Bederna Z, Szadeczky T. Cyber espionage through Botnets. Security Journal. 2020 Mar;33(1):43-62.

[213] Nyangaresi VO, Ahmad M, Alkhayyat A, Feng W. Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Systems. 2022 Dec;39(10):e13126.

[214] Mohamed N. Botnet Detection: A Review of Machine Learning and AI Strategies. In2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT) 2024 Jun 24 (pp. 1-6). IEEE.

[215] Akkepalli S, K S. A Survey of Novel Framework of Anomaly-Based Intrusion Detection Systems in Computer Networks Using Ensemble Feature Integration with Deep Learning Techniques. InProceedings of the 2024 16th International Conference on Machine Learning and Computing 2024 Feb 2 (pp. 200-205).

[216] Apostol I, Preda M, Nila C, Bica I. IoT botnet anomaly detection using unsupervised deep learning. Electronics. 2021 Aug 4;10(16):1876.

[217] Alauthman M, Aldweesh A, Al-Qerem A, Al Maqousi AY, Almomani A, Alkasassbeh M. Cryptographic Protocols for Internet of Things (IoT) Security Lightweight Schemes and Practical Deployment. Innovations in Modern Cryptography. 2024:431-48.

[218] Usha B, Amuthaguka D. Powering Up Security as Lightweight Crypto for Efficient IoT. In2024 Third International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT) 2024 Jul 24 (pp. 1-6). IEEE.

[219] Mohammad Z, Nyangaresi V, Abusukhon A. On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 320-325). IEEE.

[220] Al Hwaitat AK, Almaiah MA, Ali A, Al-Otaibi S, Shishakly R, Lutfi A, Alrawad M. A new blockchain-based authentication framework for secure IoT networks. Electronics. 2023 Aug 27;12(17):3618.

[221] Shin DH, Kim GY, Euom IC. Vulnerabilities of the open platform communication unified architecture protocol in industrial Internet of Things operation. Sensors. 2022 Aug 31;22(17):6575.

[222] Babun L, Denney K, Celik ZB, McDaniel P, Uluagac AS. A survey on IoT platforms: Communication, security, and privacy perspectives. Computer Networks. 2021 Jun 19;192:108040.

[223] Dhirani LL, Armstrong E, Newe T. Industrial IoT, cyber threats, and standards landscape: Evaluation and roadmap. Sensors. 2021 Jun 5;21(11):3901.

[224] Nyangaresi VO, Yenurkar GK. Anonymity preserving lightweight authentication protocol for resource-limited wireless sensor networks. High-Confidence Computing. 2023 Nov 24:100178.

[225] Xing Y, Shu H, Kang F. PeerRemove: An adaptive node removal strategy for P2P botnet based on deep reinforcement learning. Computers & Security. 2023 May 1;128:103129.

[226] Carpenter J, Layne J, Serra E, Cuzzocrea A, Gallo C. Structural Node Representation Learning for Detecting Botnet Nodes. InInternational Conference on Computational Science and Its Applications 2023 Jun 30 (pp. 731-743). Cham: Springer Nature Switzerland.

[227] Singh S, Gupta M, Sharma DK. Investigation of Sinkhole Attacks and Network Simulation on 6LoWPAN. InInternational Conference on Cryptology & Network Security with Machine Learning 2023 Oct 27 (pp. 75-94). Singapore: Springer Nature Singapore.

[228] Scanlon M, Kechadi T. The Case for a Collaborative Universal Peer-to-Peer Botnet Investigation Framework. InProc. 9th Int. Conf. Cyber Warf. Secur 2014 Mar 1 (pp. 287-293).

[229] Abood EW, Abdullah AM, Al Sibahe MA, Abduljabbar ZA, Nyangaresi VO, Kalafy SA, Ghrabta MJ. Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. Bulletin of Electrical Engineering and Informatics. 2022 Feb 1;11(1):185-94.

[230] Sarhan M, Layeghy S, Moustafa N, Portmann M. Cyber threat intelligence sharing scheme based on federated learning for network intrusion detection. Journal of Network and Systems Management. 2023 Jan;31(1):3.

[231] Apruzzese G, Andreolini M, Marchetti M, Venturi A, Colajanni M. Deep reinforcement adversarial learning against botnet evasion attacks. IEEE Transactions on Network and Service Management. 2020 Oct 16;17(4):1975-87.

[232] Alotaibi A, Rassam MA. Adversarial machine learning attacks against intrusion detection systems: A survey on strategies and defense. Future Internet. 2023 Jan 31;15(2):62.

[233] Kim J, Camtepe S, Baek J, Susilo W, Pieprzyk J, Nepal S. P2DPI: practical and privacy-preserving deep packet inspection. InProceedings of the 2021 ACM Asia Conference on Computer and Communications Security 2021 May 24 (pp. 135-146).

[234] Lysenko S, Bobrovnikova K, Gaj P, Savenko O. DNS-Based Fast-Flux Botnet Detection Approach. InInternational Conference on Information and Communication Technologies in Education, Research, and Industrial Applications 2021 Sep 28 (pp. 410-424). Cham: Springer International Publishing.

[235] Zhao Y, Qu Y, Xiang Y, Uddin MP, Peng D, Gao L. A comprehensive survey on edge data integrity verification: Fundamentals and future trends. ACM Computing Surveys. 2024 Oct 7;57(1):1-34.

[236] Subhash P, Qayyum MO, Mehernadh K, Sahit KJ, Varsha CL, Hardeep MN. Risk assessment threat modelling using an integrated framework to enhance security. J. Theor. Appl. Inf. Technol. 2024 May 15;102:3857-67.

[237] Pasdar A, Koroniotis N, Keshk M, Moustafa N, Tari Z. Cybersecurity Solutions and Techniques for Internet of Things Integration in Combat Systems. IEEE Transactions on Sustainable Computing. 2024 Aug 14.

[238] Jin B, Kim E, Lee H, Bertino E, Kim D, Kim H. Sharing cyber threat intelligence: Does it really help?. InProceedings of the 31st Annual Network and Distributed System Security Symposium (NDSS) 2024.