An analysis of war impact on Ukrainian critical infrastructure through network measurements

Rishabh Singla
Texas A&M University, USA
rishabh.singla@tamu.edu

Shreyas Srinivasa
Aalborg University, Denmark
shsr@es.aau.dk

Narasimha Reddy
Texas A&M University, USA
reddy@tamu.edu

Jens Myrup Pedersen
Aalborg University, Denmark
jens@es.aau.dk

Emmanouil Vasilomanolakis
Technical University of Denmark, Denmark
emmva@dtu.dk

Riccardo Bettati
Texas A&M University, USA
bettati@tamu.edu

***Abstract*—The ongoing Russia-Ukraine war has inflicted severe damage on both the geographical and the cyber landscape of Ukraine. The cyberspace of Ukraine continues to be degraded by deliberate physical and cyber warfare. Recent research shows that the degradation of the Ukrainian network correlated with the presence of Russian troops in the region and deliberate attempts of defacement attacks on certain Ukrainian websites. In this work, we examine the Ukrainian IP space by actively scanning for critical infrastructure on two protocols and observe the degradation caused by the war. We follow a measurement-based approach to map the timeline and characterize the impact by performing an analysis with a correlation of multiple datasets that include newsfeeds, disclosures from Ukrainian CERT, and NGOs. Furthermore, we correlate the data from our scans with the open datasets from Internet scanning services to discover misconfigured services and identify them using passive fingerprinting techniques. As a part of ethical considerations and responsible disclosure, we deliver our findings to the respective authorities in Ukraine through collaboration with an NGO to prevent further exploitation of misconfigured services.**

***Index Terms*—critical systems, network measurements, war**

I. Introduction

The prevailing war in Ukraine has entailed large-scale destruction both on its geographical and cyber landscape. Many services, including critical environments, leverage the Internet to provide communication and telemetry, facilitating seamless operations. The warfare that initially was reported to be only physical has now progressed to show indications of hybrid warfare that involves cyber warfare [1]. Ukraine has one of the largest energy markets in Europe and has electricity generation from hydro, thermal, and nuclear sources [2], [3]. Mission critical systems in Ukraine have been targeted in the past and attributed to Russian APTs [4]. Forensic analysis of an attack in 2015 that targeted the power grid of Ukraine shows that the events were carefully planned and executed [5]. The attack caused a service disruption of up to six hours that impacted over 230,000 consumers [6]. In the ongoing war, some of the energy sources have been deliberately targeted by Russia to cause disruption of critical services and gain a strategic hold [7]. Energy services form the backbone of society and are crucial for daily life. A degradation in critical services like the energy sector can lead to disruption in both private and commercial sectors, entailing economic consequences.

Operational Technology (OT) environments leverage Industrial Control Systems (ICS) to manage and automate the infrastructure in mission-critical environments like power plants, manufacturing units, water distribution plants, and sewage treatment plants. The ICS further uses protocols like Modbus, DNP3, PROFINet, Fieldbus, and BACNet to communicate between logical controllers and monitoring systems that facilitate control of industrial machinery. A misconfiguration of these services can compromise the ICS environment, leading to critical threats. Some misconfigurations include improper security settings that may leave the systems connected or accessible through the Internet. Studies reveal increased attacks on the ICS infrastructure and reconnaissance scans targeting protocols such as Modbus [8]. Recent research reveals many misconfigured services on the Internet that can be exploited to perform large-scale attacks [9].

Although adversaries are known to use reconnaissance processes to find vulnerable systems that can be exploited, many benign scanning services (e.g., Shodan, Censys, Shadowserver) constantly probe the Internet to monitor and report misconfigured services to prevent potential misuse [10]–[12]. In this work, we follow a measurement-based approach to determine the impact of war in Ukraine by analyzing the trends in the number of services observed during our daily Internet scans. In particular, we concentrate on the Modbus and DNP3 protocols used in ICS environments. To the best of our knowledge, our work is the first to constructively combine the results from Internet scans to assess the impact of war on critical services in Ukraine. Our motivation behind this work is to better understand the impact of war on Internet-connected infrastructure. We summarize the contributions from our work as follows:

- We scan and observe the Ukrainian IPv4 space for two protocols used in critical infrastructure over six months for capturing the measurements
- We perform a comprehensive analysis to gain insight and showcase the impact in prominent regions
- To enrich our findings, we correlate our analysis with the

978-3-903176-58-4 ©2023 IFIP

insights from datasets gathered from multiple sources like news feeds, official disclosures, and from an NGO

The rest of the paper is structured as follows. Section II provides an overview of related work outlining the cyber warfare in Ukraine and measurement-based studies. In Section III we describe the methodology of our work. We present the findings from our analysis in Section IV and discuss specific events, ethical considerations, limitations, and implications of our work in Section V. We conclude in Section VI.

II. Related Work

This section discusses the related work on studies of cyberattacks on critical infrastructure in Ukraine and measurement-based approaches for assessing and characterization endpoints.

A. Studies on cyberattacks on critical infrastructure

Serpanos et al. term the current war in Ukraine a "hybrid war" as it involves both physical and cyber warfare [1]. The authors state that cyberattacks in Ukraine are not exclusive to war and outline the history of cyberattacks as early as 2008 with the Snake cyberespionage campaign. The authors emphasize the need for analyzing and evaluating tools and methods of cyberwarfare operations and taking the necessary measures to avoid weaknesses and exploitation. Baezner et al. provide a detailed "Hotspot" analysis of historical cyber events in Ukraine from 2007 to 2017. This analysis aimed to understand threat actors' dynamics and mode of operation in target regions. The authors analyze how individual and institutional victims were affected by cyberattacks and how they responded. Furthermore, the authors suggest using the work as a basis for a comparative study of various Hotspots that can be leveraged to raise awareness on improving defenses in other states [13]. Lewis et al. propose a metric for cyberattacks and provide an overview of cyber warfare in Ukraine [14]. The author suggests looking at three important factors of creating confusion, shaping opinion, and inflicting damage to data or services as a metric for assessing the impact of cyberattacks.

Bateman et al. provide an empirical overview of the military effectiveness of Russia's wartime cyber operations in Ukraine [15]. A major purpose of this paper is to help bridge the divide between cyber-specific and general military analysis of the Russia-Ukraine war. The paper hypothesizes that the Russian wartime cyber operations have no greater strategic impact. The author argues that most of the research produced in this area is made by cyber specialists with limited knowledge of military operations, hence creating a gap. Furthermore, the author states that the main intelligence gathering has been the primary goal, not targeted attacks from Russian cyber operations.

B. Measurement-based studies

Jain et al. present an analysis of the Internet resilience in Ukraine observed over 54 days of war using the Measurement Lab's Network Diagnostic Tool [16]. From the analysis, the authors notice a network degradation in terms of average packet loss rates increasing by as much as 500% relative to pre-wartime baselines in some regions, which was further in line with the intensity of the degradation correlated with the presence of Russian troops in the region. Furthermore, the authors observe an increase in path diversity and significant changes to routing decisions at Ukrainian border Autonomous Systems (ASes) post-invasion. The work from Jain et al. suggests the war's impact on Ukraine's network infrastructure and that there was a significant observation of service degradation.

Mirian et al. conduct a measurement-based study to scan the Internet for exposed ICS infrastructure [17]. The study involves scanning the Internet for five common ICS protocols that include Modbus and DNP3 to find a total of 60K devices. The authors use the ZMap tool and perform additional probing to retrieve the description of the scanned hosts. Similarly, the authors scan for Internet-exposed DNP3 services and observe interesting results of vulnerable instances deployed on the power grid. Trestian et al. introduce a novel approach for profiling and classifying endpoints by implementing and deploying a Google-based profiling tool, which accurately characterizes endpoint behavior by collecting and strategically combining information freely available on the web [18]. The authors aim to solve the challenges in endpoint profiling using passive probing techniques, i.e., relying primarily on indexed Internet search engines like Google. The tool is evaluated with IP addresses as search keywords and adding step-wise classifications to the information gathered. Our methodology employs a similar approach by collecting metadata from public Internet-scanning services and Threat Intelligence databases. This process assists us in improving our endpoints profiling and identifying false positives.

In a more measurement-based approach, recently (January 2023), Belson et al. presented an analysis of Internet disruptions for the last quarter of 2022 [19]. The authors present similar analyses for the year, distributed over quarters. The report from the first quarter indicates two significant disruptions in March 2022 caused by a severe cyberattack on Ukrtelecom [20]. From an overview of the related work, we summarize that much work provides insight into the cyber warfare in Ukraine and some measurement-based studies that present the impact and strategy of cyber warfare. We take this as motivation to try assessing the impact and implications of the war in Ukraine on critical infrastructure through a measurement-based study that involves analyzing the data received from Internet-exposed services and correlating the events.

III. Methodology

In this section, we outline the methodology followed in our approach. The study is divided into two periods: the first period from March-August 2022 and the second from October-December 2022. While we initially planned to end the study after the first phase, we started observing interesting trends and events at the beginning of October. We hence decided to continue with our methodology and further analyze the data. Figure 1 presents an overview of the steps in our methodology that include Internet-wide scanning, metadata collection, fingerprinting, noise filtration, IP reputation check, and the event correlation process. We describe each process in the following sections.

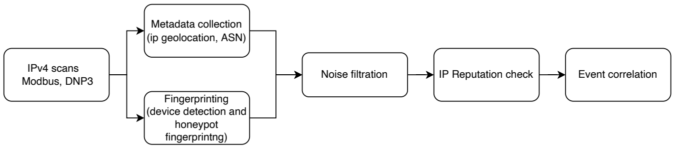

Fig. 1. Overview of steps in methodology

A. Internet-wide Scanning

Our methodology relies on the results obtained from Internet scanning. The Internet scanning process was performed daily over the Ukrainian IPv4 space. We obtain the subnet list from the RIPE Database [21]. We limit our scan to 2193 ASNs and 3058 IPv4 subnets and follow the scanning blocklists suggested by IANA IPv4 special-purpose address registry [22]. The scans were performed with the ZMap [23] Internet scanning tool with some customization to avoid stress on the scanned instances. We mainly scan two protocols, Modbus [24] and DNP3 [25], extensively used in OT and mission-critical environments. The Modbus protocol was scanned with port 502, and DNP3 was scanned with port 20000. While the DNP3 protocol can run on either TCP or UDP, we chose to run our scan on both protocols in TCP.

B. Metadata collection

The Internet scanning process provides IP addresses that respond to our scanning probes. As previously mentioned, the scanning probes are designed to obtain minimal information about the end system. We collect metadata to get insights into the IP addresses received from the scan, such as geographical location (by city and region), ASNs, and *whois* information. The metadata helps filter false positives like IPs that are not geographically located in Ukraine. Initially, the IP to geolocation metadata is obtained from the MaxMind GeoLite2 City database [26] that lists an average of 55% accuracy at the country level. To further improve the filtration, we obtain geolocation from the IPAPI service [27] that claims an accuracy of 60% at the region level. We aggregate the data from both data providers to enrich the data. The ASN and *whois* information is obtained from the DomainTools *whois* data API [28]. Lastly, to further enhance the accuracy we perform a random sampling of corresponding websites and other publicly facing servers to verify that the IP addresses belonged to Ukraine-based entities.

C. Passive fingerprinting and noise filtration

The noise removal process aims to filter the false positives from the results obtained from the scanning process. The noise could be from other services running on identical ports, honeypots [29], or even IPs not geolocated from Ukraine. First, to filter the non-relevant systems i.e., other services running on ports 502 and 20000, we collect additional metadata from Internet-scanning databases like Censys and Shodan [10], [11]. Upon aggregating this data from the metadata obtained from the previous steps, we determine if the device is running the Modbus or DNP3 service. Note that the scanning services have a limited scope and may not contain information on some IPs. Second, to filter honeypots (fake, simulation-based systems deployed to trap malicious actors), we use the work from [30] that provides a multistage fingerprinting approach. We use the approach to fingerprint Conpot, a medium-interaction honeypot that can simulate ICS protocols [31]. Lastly, to filter the IPs that are not geolocated in Ukraine, we use the geolocation metadata aggregated from the previous step from MaxMind, IPAPI, and *whois* databases. The data is now enriched with metadata and filtered from noise.

D. Preliminary Analysis and Reputation checks

After the metadata collection and the noise filtering process, the resulting dataset is prepared for deeper analysis by normalization. In this phase, we query the dataset to count systematically, identify redundancies, and group data based on relevance, interest, and order. Through the preliminary analysis, we get the initial results and identify data points of interest. We further perform a reputation analysis of the IP addresses observed with suspicious trends to check if they were involved in malicious events like DDoS attacks, with the possibility of being compromised. The IP reputation is checked with services like Greynoise, AbuseIP, and Virustotal that provide information on malicious activity from an IP address [32]–[34]. We present the findings from preliminary analysis in Section IV. Furthermore, through the initial analysis, we observe some interesting anomalies discussed in Section V.

E. Event correlation

After the preliminary analysis of the dataset, we find some interesting trends. The war has a wide-scale impact that spans many regions of Ukraine and to better understand and identify any related causal effects, we correlate the interesting data points from the analysis to known events tagged to the affected regions. For example, the Russian forces bombed the Zaporizhzhia plant in southeastern Ukraine on March 4, 2022 [7]. We observe from our dataset that on this day, there is a clear downward trend in the number of IPs seen online in that region. The correlation of the events with our dataset provides better reasoning for the trends observed in our dataset. Furthermore, this process helps in establishing factors that help illustrate the possible impact on the region. This step is crucial in our methodology as it forms the core of our contribution. We correlate our findings with several data points from the news media and a dataset from the CyberPeace Institute (NGO) [35].

IV. Analysis

In this section, we present our findings from the Internet-wide scanning, noise filtering, analysis, and the relevant events reported in affected regions.

A. Internet scanning

Figure 2 presents the total number of unique IPs seen during the scanning period for Ukraine. The scanning activity was carried out in two phases. The first phase was carried out in March-August 2022 and the second phase from October-December 2022 (Indicated by a blue line on all figures). We observe a steady trend in the first phase in comparison to a lot of turbulence seen over the second phase of scanning. A few substantial drops during the end of March may be possibly attributed to network outages. We cannot certainly attribute this because of the absence of ground truth and we did not find any particular attack on the infrastructure during this period. This downward trend during March is observed in the scanning results across all the cities of Ukraine. A total of $435,300$ DNP3 and $429,650$ Modbus unique IPs were observed through the scanning period.

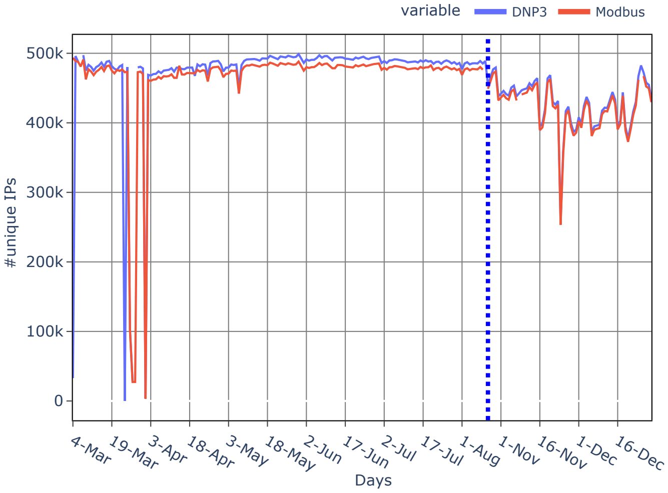

Fig. 2. Total Unique IPs (Ukraine) observed by day during the year 2022

B. Passive-fingerprinting

The scanning process provides a list of IP addresses that have the corresponding open ports on the target host. However, it does not check if the hosts with open ports are running specific services. To identify and filter false positives, either additional probing techniques like active fingerprinting or metadata-based analysis like passive fingerprinting can be leveraged. Since active fingerprinting requires additional probing that may lead to ethical complications, we avoid sending further probes to the target system. Instead, we use some passive fingerprinting techniques that leverage the metadata. We describe the methods and the results of the noise reduction process below.

1) Cross-validation with Internet-scanning services: The IP address from the scan results is cross-validated with Internet-wide scanning service engines Shodan [10] and Censys [11]. The scanning services contain metadata about IP addresses like open ports, hostnames, ASN, and banner-related information that can help in determining false positives. We check all the IP addresses from our scan results to eliminate potential noise. Figure 3 shows the number of false positives identified by validation through scanning services. We discover a large number of IPs from our results that are running other services on ports 502 and 20000. Among these, we find most of them to be routers that may be misconfigured or port-forwarded for accessibility from the Internet.

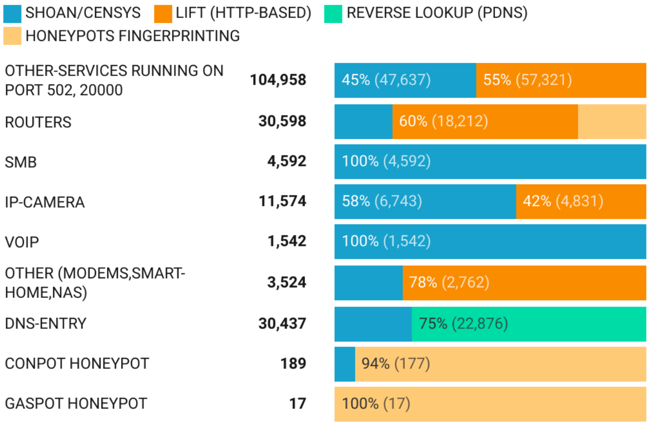

Fig. 3. Summary of noise filtering by Passive fingerprinting

2) HTTP-based fingerprinting: We leverage the open-source low-impact fingerprinting tool *Lift*[1] to fetch HTTP banners for automated analysis. The *Lift* fingerprinting tool sends HTTP requests to the target system and on receiving a response, the headers are parsed to determine the end system. The results from the passive-fingerprinting process on the web services can be seen in Figure 3. We identify and filter a large number of devices to be routers and IP-Cameras by parsing the response headers.

3) DNS check: Our scan results show both consistent and turbulent behavior of hosts. We perform reverse-domain lookups to determine the sporadic assignment of these public IPs. The lookup results help identify if the host continues to be in the previous domain or has been reconfigured. We use *DNSDB*, a passive DNS (pDNS) historical Internet database to find any historical changes on the domain assignment to an IP address [36]. The DNS check is performed over a sample of hosts that are observed to be turbulent in the scanning results. Figure 3 shows the results of DNS checks on sample sizes taken from multiple regions. We filter the IP addresses that resolve to an FQDN (fully qualified domain name) as it is unlikely that a service running in critical infrastructure to resolve to an FQDN.

4) Honeypots detection: Honeypots are deception-based systems that emulate a target system or service. They are used as a proactive measure to detect any suspicious traffic toward a target system or network. The presence of honeypots in our scan results poses false positives. Honeypot fingerprinting is the process of determining if the end-system in interaction is a honeypot. We concentrate on fingerprinting honeypots that simulate Modbus and DNP3 services. In particular, we focus to identify Conpot [31], a medium-interaction honeypot

[1] https://github.com/trylinux/lift

capable of simulating both Modbus and DNP3 services, and Gaspot [37]. Furthermore, we use metadata-based techniques that use information from public sources about the target to determine if it is a honeypot [30]. Figure 3 shows the number of honeypots detected from our scan results using the metadata-based approach. We find a total of 206 honeypots and 6743 routers from this fingerprinting technique.

C. Region-wise results

In this section, we present the results of the scans in selected regions of Ukraine. We present our results in the following sections.

1) Kyiv city and Kharkhiv: We present daily trends of DNP3 and Modbus IPs in Kyiv and Kharkiv cities in Figure 4. We observe that in both of these cities, the overall major disruptions are in phase 2, whereas phase 1, did see some drops during certain time periods. We suspect these disruptions could either be physical attacks or cyberattacks on critical infrastructure. One of the major drops in these trends could be attributed to the strikes on critical infrastructure on Nov 24, 2022. As per a report from [38], we observe downward trends in scan results of Kyiv, Lviv, and Odesa that could be a result of power outages due to the cyberattack.

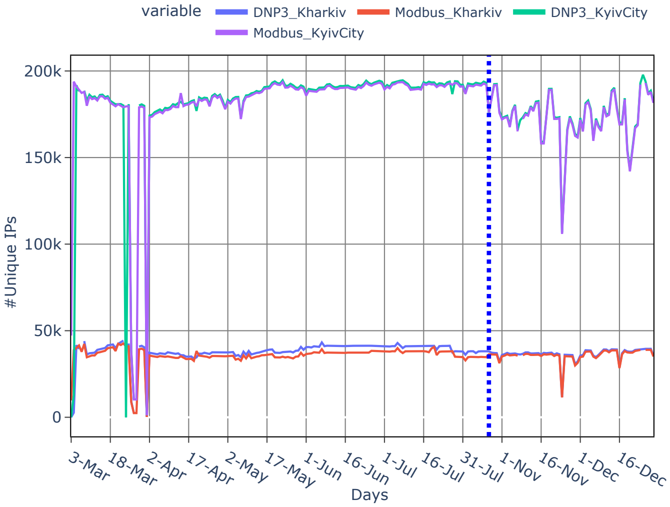

Fig. 4. Kyiv City and Kharkiv (Year: 2022)

2) Kherson: Figure 5 shows Kherson City in the Kherson region. We point out some of the incidents which match the trends from the figure. On 23 March 2022, counterattacks were launched by Ukrainian forces against Russian forces in Kherson Oblast. A significant drop was observed during May 1-4 which aligns with the Internet connectivity issues reported by Cloudflare in the Kherson region [39]. A gradual drop is observed starting from June 1, 2022, which aligns with the announcement shared by the Governor of Mykolaiv Oblast (Kherson City) about the demolition of bridges near Kherson by Russian forces, and the trends kept on to be low. Russia has still control over this region latest reported on November 4, 2022, [40]. The Ukrainian forces gained back control of Kherson post-November and we observe consistent trends in Figure 5 during this period.

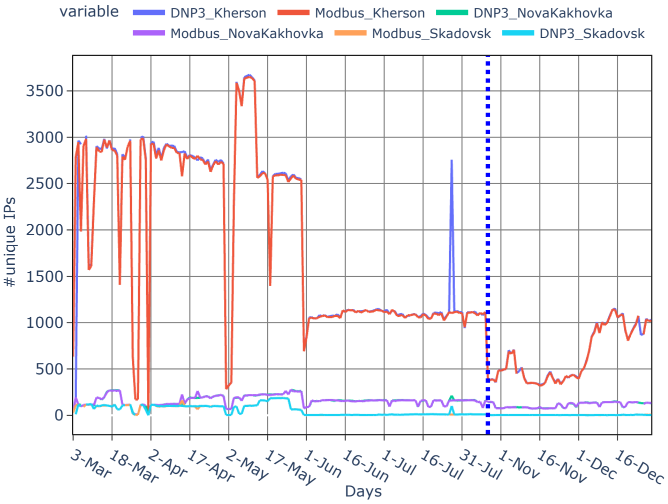

Fig. 5. Kherson region (Year: 2022)

3) Donetsk: Figure 6 presents some trends of active IPs over time across the top three cities under the Donetsk region. Mariupol city shows a very different trend among all. The invasion at Mariupol began on Feb 24 in the city and on March 12, it was partially captured by Russia [41]. On May 19, 2022, the tensions subsided and the city was under the control of Russia [42]. Following the takeover, the critical infrastructure seems to be revived slowly with more than 15000 devices observed latest until the end of December.

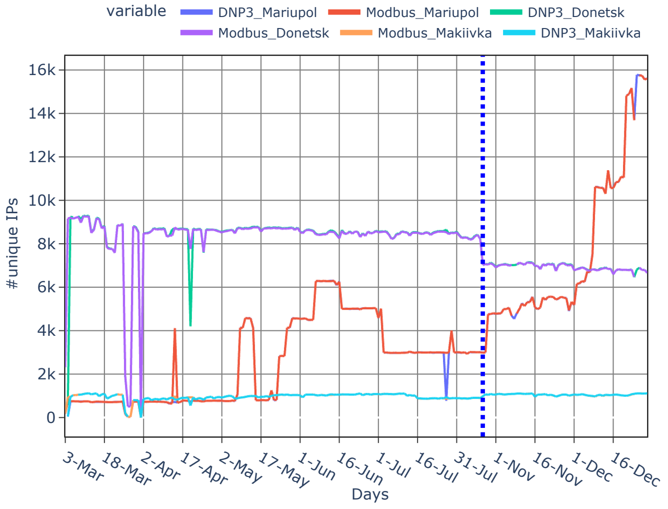

Fig. 6. Donetsk Oblast (Year: 2022)

4) Chernihiv: Figure 7 shows the top three cities from the Chernihiv region. A pumping station was bombed on 14 March 2022, bridges were destroyed on March 25, and libraries were bombed on March 30 [43]. However, on April 1, the Ukrainian government declared that Russian forces have withdrawn from Chernihiv. We observe continuous upward trends following the attack period.

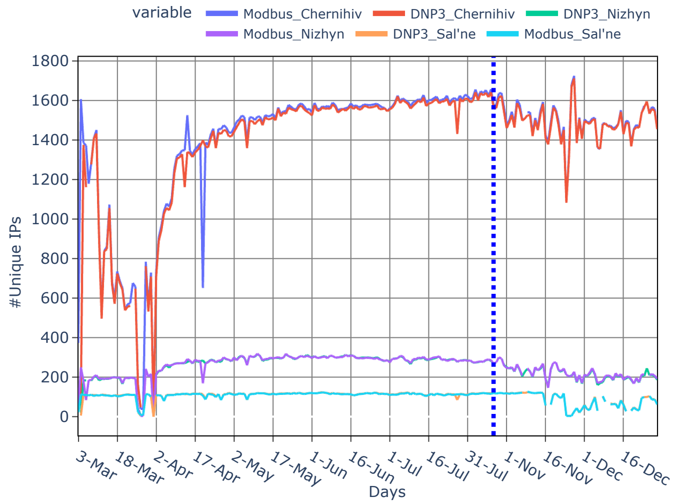

Fig. 7. Chernihiv Oblast (Year: 2022)

5) Kyiv: Figure 8 presents the top four cities from the Kyiv region. The city of Irpin shows a sudden jump from April 19 to June 23 and again a big drop. Boryspil city also shows a big drop between March 12 to 16 and then a spike between April 06 to May 03. According to [44], there were several attacks made on the airport in Boryspil.

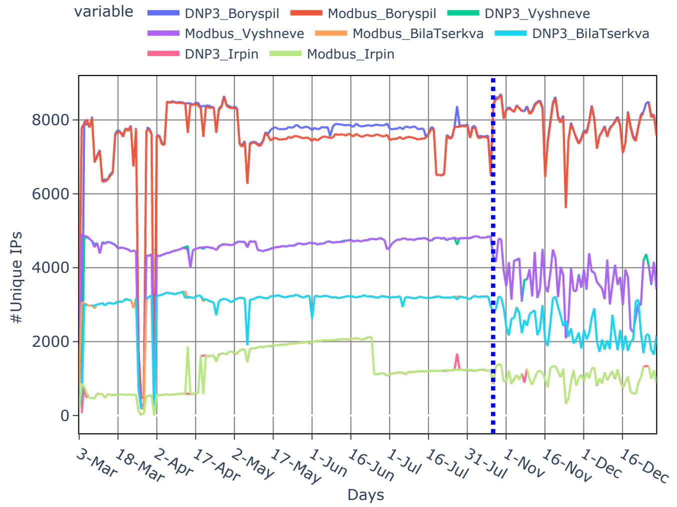

Fig. 8. Kyiv Oblast (Year: 2022)

6) Enerhodar: Figure 9 shows the city Enerhodar (The biggest Nuclear Plant in Asia) and a thermal power plant. We observed interesting trends which match with a report published on events/attacks happening on the nuclear plants by the Russian army in Enerhodar city. For example, the drop observed on March 04, 2022, may be a result of the impact of Russian armored vehicles and tanks that approached the plant [45]. Russia was controlling the plant since March 12, 2022. On April 16, missiles were recorded over the plant risking physical integrity. On September 17, the Nuclear plant again connected Ukraine's national power grid.

7) Mykolaiv: Figure 9 presents trends from the city of Mykolaiv in the Mykolaiv region. Before April 8, 2022, when Russian forces were pushed back from this region, quite a few turbulent trends have been observed [46]. For example, on March 18, two Russian missiles were reported to strike this region.

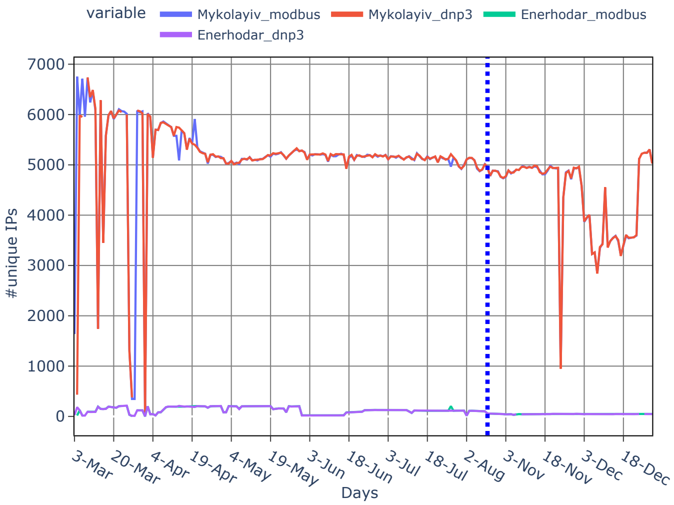

Fig. 9. Mykolaiv and Enerhodar City (Year: 2022)

D. Specific observations in the second phase of study

In this section, we explain some of the notable trends and the correlated events from the second phase of the study conducted between September to December 2022.

1) Oct 31, 2022: The Russian Armed Forces launched more than 50 missiles at energy infrastructure in Kyiv, and other regions of Kharkiv, Zaporizhzhia, Cherkasy and Kirovohrad [47]. The missile impacted up to 18 facilities that left 40% of Kyiv residents without power and 270,000 apartments without electricity. This impact can be observed in Figure 4.

2) Nov 15, 2022: On 15 November 2022, Russia launched a wave of missiles at several Ukrainian cities that led to severe power and water shortage [48]. The affected cities include Kyiv, Lviv, Zhytomyr, Kryvy Rih and Kharkiv. The drops can be distinctly observed in Figure 4 and Figure 8. The missile strike is said to have impacted more than 10 million people without power. On November 17, Ukrainian officials reported that electricity had been fully restored.

3) Nov 24, 2022: We observe one of the biggest drops among the scan results of both Modbus and DNP3 during 23-24 November, which aligned with a targeted kinetic (missile) attack on the energy infrastructure of Ukraine [49]. The Russian military launched missiles at civilian settlements and energy infrastructure, although most of those were said to have been shot down. The attack caused blackouts over much of Ukraine and forced several nuclear power plants to shut down. The impact of the attack can be observed in Figure 4.

4) Dec 05, 2022: Russia launched a renewed wave of missile strikes against Ukraine, consisting of about 70 cruise missiles [50]. Ukraine claimed 60 missiles have been shot down, and Russia claimed 17 targets have been hit on the ground. Moscow has been targeting Ukraine's power grid in intense waves of attacks since October, and state energy company Ukrenergo, which operates the national power grid, said more infrastructure had been hit. Prime Minister Denys Shmyhal later said energy facilities had been hit in the regions of Kyiv, Vinnytsia in west-central Ukraine, and Odesa in the south, but that Ukraine's energy system was still functioning. The impact can be observed in Figure 4 and Figure 6.

5) Dec 16, 17 and 19 2022: Russia launched around 76 missiles on Kyiv, Kharkiv, Poltava, and Kremenchuk, destroying infrastructure. These 76 missiles were fired at 9 power plants; Ukraine claims 60 were intercepted [51]. Missiles were launched targeting infrastructure in Kyiv, Kharkiv, Kryvyi Rih, and Zaporhizhzhia. Kyiv council member Ksenia Semenova stated that approximately 60% of residents were without power and 70% were without water. Ukraine restored power and water to approximately 6 million residents in 24 hours. The impact can be observed in Figures 4 and 9. According to the Ukrainian Air Force, on December 19, Russia attacked Ukraine's infrastructure with 35 Iranian Kamikaze drones, 30 of which are said to be shot down [52]. An infrastructure facility was damaged, leaving three areas in Kyiv without a power supply. Energy shortages caused interruptions in heat and water supply. Mykolaiv and Kherson regions were also attacked. The building of the Kherson Oblast State Administration was partially destroyed. The impact can be observed in Figures 4 and 5.

6) Dec 29, 2022: Ukraine Presidential advisor Mykhailo Podolyak stated that over 120 missiles were launched at infrastructure facilities in Kyiv, Kharkiv, Lviv, and Odesa [53]. Ukraine claimed that 54 of 69 missiles were shot down and left 40% of Kyiv without power. The impact can be observed in Figures 4 and 8.

E. IP Reputation

The IPs revealed from our Internet scan are services that were exposed either deliberately or misconfigured. To assess if these IPs were exploited and leveraged by cyberattacks, we perform a reputation check. We check the IPs from the results with popular IP reputation check databases like AbuseIPDB [34], Greynoise [32], and Virustotal [33]. We classify an IP to be malicious if we find any malicious tags on them on either IP-databases. Furthermore, we identify the potential participation of these Ukrainian IPs in cyberattacks by correlating the information obtained from these databases and other datasets from our analysis. Figure 10 shows the percentage of IPs classified by type and source. We observe diverse types of malicious IP sources ranging from worms, malware, brute-force attempts, and reconnaissance probes.

V. Discussion

In this section, we discuss the eminent observations and correlations observed from our analysis. We further discuss the ethical considerations and limitations.

A. Kinetic and Non-Kinetic strategies

Here we discuss the possibility of Russian non-kinetic attacks, such as cyber-attacks and information attacks to disrupt critical infrastructure [54]. There have been multiple instances of Russian cyber attacks on Ukrainian infrastructure before the start of the war in February, but they were not successful in impacting the critical infrastructure [54], [55]. Russians attempted multiple cyber attacks in Mariupol before launching missile attacks, which we suspect to be a strategic move to disrupt the city before launching more costly kinetic attacks.

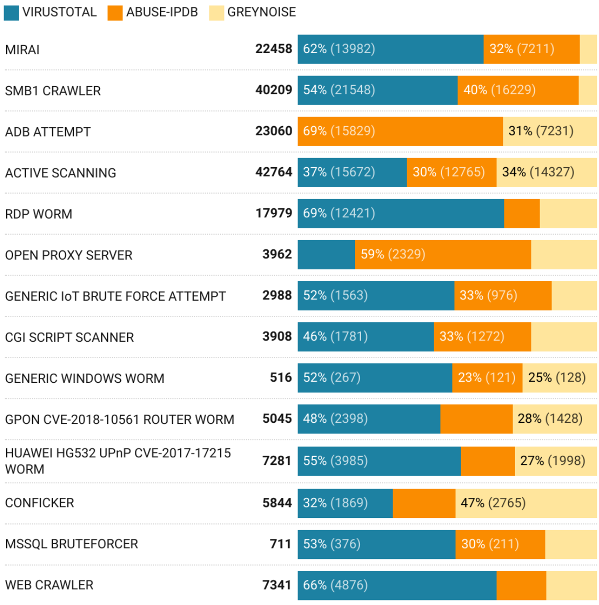

Fig. 10. Malicious IPs, Classified by Type and Database source

B. Eminent observations

1) DDoS attack against Ukraine postal service: As per the cyberattack dataset from the NGO we collaborated with, Ukraine postal services were hit by a DDoS Attack by Russians on April 21, 2022, following the release of a particular stamp challenging Russian soldiers [35], [56]. Upon IP reputation analysis of our dataset, we observed 2 Ukrainian IPs involved in this attack.

2) Mariupol Invasion Trends: We discuss the strategic importance of Mariupol, a Ukrainian city targeted by Russian forces to create a land corridor and block Ukrainian exports [57]. Fig 11 represents a heatmap of all the observed Modbus IPs in Mariupol, where the yellow color suggests the Modbus device is active and the other colors show the device is not detected. We notice a sudden increase in active IPs on April 14, when the bombing was temporarily halted to allow for humanitarian evacuations [58]. Our data provide a fact check on the claim of Russian soldiers invading the Azovstal Iron and Steel Works complex on May 4 refuted by Ukrainian soldiers [59]. We see more number of IPs active during that time period. On May 16, the city was captured by Russian forces, and after the war, the number of devices in the area increased, matching the claim made by Russians that they will be rebuilding Mariupol [60].

3) Kinetic Attack on Odesa City: On December 10, Russia used Iranian-made drones to attack two energy facilities in Odesa, leaving the port and 1.5 million people without power [61]. Our data validate this strike as we observed a sudden

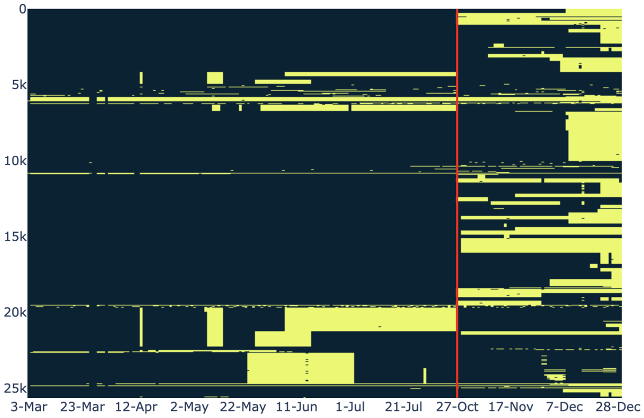

Fig. 11. Mariupol Heatmap of modbus IP active daywise (Year: 2022)

decrease in the number of Modbus and DNP3 devices in Odesa, as shown in the highlighted region in Figure 12, while Kyiv, which is close to Odesa, did not experience a similar decrease during the same time. We highlight this incident to show the authenticity of our dataset.

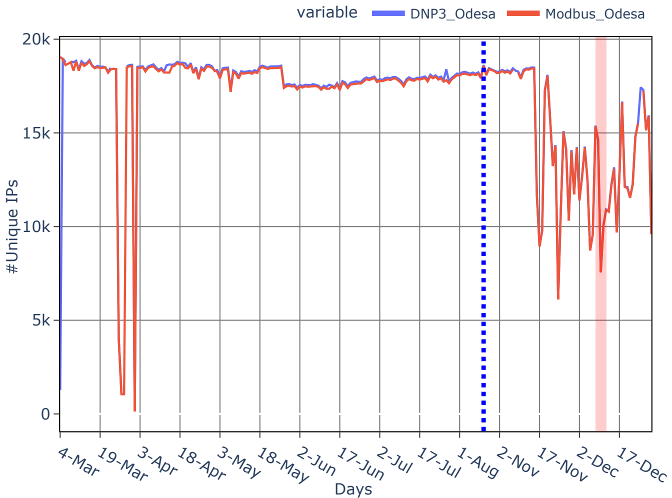

Fig. 12. Odesa Trend: Kinetic attack on Dec 10, 2022

C. Ethical Considerations

We follow a measurement-based approach to assess the impact of war by analyzing the data from Internet scans on two protocols used in critical infrastructure environments. In this section, we address the ethical considerations followed in our work. Our methodology uses the results of Internet scanning to find misconfigured Modbus and DNP3 services exposed to the Internet. We follow the following guidelines to ensure we are ethical in our scanning approach.

First, the scanning probes are modified to ensure that they do not impact the availability of the end system and trigger a minimal response. Second, we operate a webserver on our scanning instance which states information about us and the research, with the possibility of opting out from our scans. We did not receive any requests for opting out. Third, we acknowledge that the results from the Internet scan can be considered critical and can be abused if it is made public. We ensure that the list of results from our scans is not publicly shared and carefully store the data in a controlled database for further processing. We want to emphasize that our work is focused on assessing the impact and not being a cause for the impact ourselves. To ensure this, we collaborated with CyberPeace, an NGO that helped us make responsible disclosure of the IPs to respected authorities in Ukraine [35].

D. Limitations

The Internet scans are concentrated on the Ukraine subnets as listed on the RIPE database [21]. However, on the aggregation of data with the metadata, we observed outliers based on geolocation and ASNs. We acknowledge the limitations caused by false positives due to inaccuracy in geolocation tagging. The IP-to-geolocation mapping databases referred to in our work have an accuracy of 55-60%. This limits the validation of the results, accuracy, and further filtering of false positives. The trends presented in our analysis can be skewed because of IP churning or blocklisting of our probes. While IP churning is viable due to challenging networking scenarios and failover configurations, we acknowledge that our probes may have been blocked. The fingerprinting analysis from our methodology has a limited scope. The fingerprinting process could be enhanced by collaborating with respective entities from Ukraine. While we tried to find possible collaborators to enhance this process, it was difficult to engage due to the challenging ground situation and communication. The IP reputation data are based on community ratings and observed events. These reputations can be skewed and the possibility of a wrong reputation is possible. Our data and others [15] suggest Ukraine's Internet connectivity did not impact our results considerably. Lastly, our impact analysis is based on the possible correlation between trends and events. This analysis represents a subset for illustrating the impact and cannot be considered for total representation.

E. Implications

The analysis of the scanning data and the correlation provide interesting insights. First, the results from the Internet-wide scans reveal misconfigured Modbus and DNP3 services exposed to the Internet. This entails that a large number of systems can be potentially abused or exploited for malicious purposes. It is necessary to patch these services to reduce the attack surface. Second, the observations from our analysis reveal an increasing importance of digitalization and more importantly the resilience of critical infrastructure towards cyber threats and kinetic attacks. We observe clear trends from our scanning data that suggest that most of the affected critical infrastructure was restored in a matter of days. Third, the timeline of events represents an emphasis and strategy that includes having a competitive edge through cyber dominance.

VI. Conclusion

In this work, we scan the Ukrainian IPv4 space on a daily basis for Modbus and DNP3 protocols mainly used in critical infrastructure for a period of over 6 months. The results from the scans are further analyzed to study the impact by mapping and correlating the events from many datasets. We follow a measurement-based approach and analysis to present the impact of war. Our work suggests that network measurements can be used to validate the ground truth in dynamic situations when conflicting information may be arriving from multiple sources. As a part of future work, we aim to perform an in-depth analysis of the datasets to understand the severity of the damages caused particularly by cyberattacks.

Acknowledgment

This Research is supported by a T3 Grant from Texas A&M University, an NPRP Grant NPRP12C-0814-190012 from the Qatar National Research Fund (a member of the Qatar Foundation), and NSF Project 2331767. The findings achieved herein are sorely the responsibilities of the authors.

References

[1] D. Serpanos and T. Komninos, “The cyberwarfare in ukraine,” *Computer*, vol. 55, no. 7, pp. 88–91, 2022.

[2] I. E. Agency, “Ukraine energy profile,” 2020. [Online]. Available: https://www.iea.org/reports/ukraine-energy-profile

[3] W. N. Association, “Nuclear power in ukraine.” [Online]. Available: https://world-nuclear.org/information-library/country-profiles/countries-t-z/ukraine.aspx

[4] M. J. Assante, “Confirmation of a coordinated attack on the ukrainian power grid,” *SANS Industrial Control Systems Security Blog*, 2016.

[5] D. U. Case, “Analysis of the cyber attack on the ukrainian power grid,” *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, pp. 1–29, 2016.

[6] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, “A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services,” *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3453–3495, 2018.

[7] W. N. Association, “Russia-ukraine war and nuclear energy.” [Online]. Available: https://world-nuclear.org/information-library/country-profiles/countries-t-z/ukraine-russia-war-and-nuclear-energy.aspx

[8] C. Fachkha, “Cyber threat investigation of scada modbus activities,” in *2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 2019, pp. 1–7.

[9] S. Srinivasa, J. M. Pedersen, and E. Vasilomanolakis, “Open for hire: Attack trends and misconfiguration pitfalls of iot devices,” in *Proceedings of the 21st ACM Internet Measurement Conference*, ser. IMC ’21. New York, NY, USA: Association for Computing Machinery, 2021, p. 195–215. [Online]. Available: https://doi.org/10.1145/3487552.3487833

[10] SHODAN, “Shodan,” 2022. [Online]. Available: https://www.shodan.io/

[11] Censys, “Censys search,” 2021. [Online]. Available: https://censys.io/

[12] S. Foundation, “Shadowserver.” [Online]. Available: https://www.shadowserver.org/

[13] M. Baezner, “Cyber and information warfare in the ukrainian conflict,” ETH Zurich, Tech. Rep., 2018.

[14] J. Andrew, K. Geers *et al.*, “‘compelling opponents to our will’: The role of cyber warfare in ukraine,” in *Cyber war in perspective: Russian aggression against Ukraine*. NATO CCDCOE, 2015, pp. 39–48.

[15] J. Bateman, “Russia’s wartime cyber operations in ukraine: Military impacts, influences, and implications,” 2022. [Online]. Available: https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657

[16] A. Jain, D. Patra, P. Xu, J. Sherry, and P. Gill, “The ukrainian internet under attack: An ndt perspective,” in *Proceedings of the 22nd ACM Internet Measurement Conference*, ser. IMC ’22. New York, NY, USA: Association for Computing Machinery, 2022, p. 166–178. [Online]. Available: https://doi.org/10.1145/3517745.3561449

[17] A. Mirian, Z. Ma, D. Adrian, M. Tischer, T. Chuenchujit, T. Yardley, R. Berthier, J. Mason, Z. Durumeric, J. A. Halderman, and M. Bailey, “An internet-wide view of ics devices,” in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, 2016, pp. 96–103.

[18] I. Trestian, S. Ranjan, A. Kuzmanovi, and A. Nucci, “Unconstrained endpoint profiling (googling the internet),” *SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 4, p. 279–290, aug 2008. [Online]. Available: https://doi.org/10.1145/1402946.1402991

[19] D. Belson, “Internet disruptions overview for q4 2022,” 2023. [Online]. Available: https://blog.cloudflare.com/q4-2022-internet-disruption-summary/

[20] ——, “Internet disruptions overview for q1 2022,” 2023. [Online]. Available: https://blog.cloudflare.com/q1-2022-internet-disruption-summary/

[21] RIPE, “Ripe database,” 2022. [Online]. Available: https://apps.db.ripe.net/db-web-ui/query

[22] IANA, “Iana ipv4 special-purpose address registry,” 2022. [Online]. Available: http://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml

[23] Z. Durumeric, E. Wustrow, and J. A. Halderman, “Zmap: Fast internet-wide scanning and its security applications,” in *22nd USENIX Security Symposium (USENIX Security 13)*. Washington, D.C.: USENIX Association, Aug. 2013, pp. 605–620. [Online]. Available: https://www.usenix.org/conference/usenixsecurity13/technical-sessions/paper/durumeric

[24] modbus.org, “Modbus technical resources,” 2023. [Online]. Available: https://modbus.org/tech.php

[25] DNP3.org, “Overview of dnp3 protocol,” 2023. [Online]. Available: https://www.dnp.org/About/Overview-of-DNP3-Protocol

[26] MaxMind, “Maxmind geoip and geolite databases and web services,” 2023. [Online]. Available: https://dev.maxmind.com/geoip?lang=en

[27] IPAPI, “Ipapi real-time geolocation & reverse ip lookup rest api,” 2023. [Online]. Available: https://ipapi.com/

[28] DomainTools, “Domaintools whois lookup,” 2023. [Online]. Available: https://whois.domaintools.com/

[29] S. Srinivasa, J. M. Pedersen, and E. Vasilomanolakis, “Interaction matters: A comprehensive analysis and a dataset of hybrid iot/ot honeypots,” in *Proceedings of the 38th Annual Computer Security Applications Conference*, ser. ACSAC ’22. New York, NY, USA: Association for Computing Machinery, 2022, p. 742–755. [Online]. Available: https://doi.org/10.1145/3564625.3564645

[30] ——, “Gotta catch ’em all: a multistage framework for honeypot fingerprinting,” 2021.

[31] L. Rist, J. Vestergaard, D. Haslinger, A. Pasquale, and J. Smith, “Conpot ics/scada honeypot,” The Honeynet Project, 2013.

[32] GreyNoise, “Greynoise.” [Online]. Available: https://greynoise.io/

[33] Virustotal, “Virustotal.” [Online]. Available: https://www.virustotal.com

[34] abuseipdb, “abuseipdb.” [Online]. Available: https://abuseipdb.com/

[35] cyberpeace, “Cyber attacks in times of conflict platform #ukraine,” 2023. [Online]. Available: https://cyberconflicts.cyberpeaceinstitute.org/

[36] F. Security, “Passive dns historical internet database: Farsight dnsdb.” [Online]. Available: https://www.farsightsecurity.com/solutions/dnsdb/

[37] K. Wilhoit and S. Hilt. (2015) The gaspot experiment: Unexamined perils in using gas-tank-monitoring systems. Black Hat. USA.

[38] M. Kathleen, N. H. Sana, S. Aditi, and V. Adrienne, “November 23, 2022 russia-ukraine news,” 2022. [Online]. Available: https://edition.cnn.com/europe/live-news/russia-ukraine-war-news-11-23-22/h_e569557fbf985c64baa88312a559f821

[39] T. João and B. David, “Tracking shifts in internet connectivity in kherson, ukraine,” 2022. [Online]. Available: https://blog.cloudflare.com/tracking-shifts-in-internet-connectivity-in-kherson-ukraine/

[40] E. Holly and M. Amanda, “Ukraine attacks russian units in kherson, saying moscow didn’t request a ‘green corridor’ for withdrawal,” 2022. [Online]. Available: https://www.cnbc.com/2022/11/10/russia-ukraine-war-updates.html

[41] Ukraine war: Heavy losses reported as battle for bakhmut rages. [Online]. Available: https://www.bbc.com/news/world-europe-64935449

[42] Deadly donetsk blasts hit separatist-run city in ukraine. [Online]. Available: https://www.bbc.com/news/world-europe-62952641

[43] Siege of chernihiv. [Online]. Available: https://en.wikipedia.org/wiki/Siege_of_Chernihiv#cite_note-62

[44] Ukraine crisis: Russian missile hits technical building at kyiv’s boryspil international airport. [Online]. Available: https://aviationsourcenews.com/news/ukraine-crisis-russian-missile-hits-technical-building-at-kyivs-boryspil-international-airport/

[45] Ukrainian nuclear power plant attack condemned as russian troops ‘occupy’ facility. [Online]. Available: https://edition.cnn.com/2022/03/03/europe/zaporizhzhia-nuclear-power-plant-fire-ukraine-intl-hnk/index.html

[46] Russia-ukraine war: Several killed in mykolaiv attack. [Online]. Available: https://www.aljazeera.com/news/2022/3/29/seven-people-killed-22-wounded-in-ukraines-mykolaiv-attack

[47] N. Kostan, V. Olga, B. Victoria, and K. Lianne. (2022) Russian missiles bombard cities across ukraine, hitting power and water infrastructure. [Online]. Available: https://edition.cnn.com/2022/10/31/europe/russian-missile-strikes-ukraine-intl/index.html

[48] K. Julia, C. Vasco, L. Tim, and N. H. Sana. (2022) Wave of russian missiles hit ukraine after zelensky outlines conditions for peace at g20 summit. [Online]. Available: https://edition.cnn.com/2022/11/15/world/kyiv-strikes-russia-zelensky-peace-intl/index.html

[49] BBC. (2022) Ukraine war: Most of kyiv spends night without power after missiles. [Online]. Available: https://www.bbc.com/news/world-europe-63740923

[50] "Ukraine war: Eighth wave of russian missile attacks," 2022. [Online]. Available: https://www.bbc.com/news/world-europe-63863138

[51] "Ukraine's second city kharkiv without power after russian strikes," 2022. [Online]. Available: https://www.bbc.com/news/world-europe-63997749

[52] (2022) Ukraine war: Overnight strikes hit kyiv as putin visits belarus. [Online]. Available: https://www.bbc.com/news/world-europe-64024992

[53] (2022) Russia fires dozens of missiles at ukrainian cities. [Online]. Available: https://www.bbc.com/news/world-europe-64114784

[54] M. Lehto and G. Henselmann, "Non-kinetic warfare - the new game changer in the battle space 316 non-kinetic warfare -the new game changer in the battle space," 03 2020.

[55] K. Flinders. (2022) Failure of russia's cyber attacks on ukraine is most important lesson for ncsc. [Online]. Available: https://www.computerweekly.com/news/252525514/Failure-of-Russias-cyber-attacks-on-Ukraine-is-most-important-lesson-for-NCSC

[56] E. b. T. H. Pavel Polityuk and A. MacSwan. (2022) Ukraine's postal service hit by cyberattack after sales of warship stamp go online. [Online]. Available: https://www.reuters.com/world/europe/ukraines-postal-service-hit-by-cyberattack-after-sales-warship-stamp-go-online-2022-04-22/

[57] L. Keay. (2022) Ukraine war: Why is mariupol so important to both sides? [Online]. Available: https://news.sky.com/story/ukraine-war-why-is-mariupol-so-important-to-both-sides-12594896#

[58] VOA. (2022) Latest developments in ukraine: April 14. [Online]. Available: https://www.voanews.com/a/latest-developments-in-ukraine-april-14-/6528961.html

[59] BBC. (2022) Ukraine war: Zelensky plea as russians seek mariupol endgame. [Online]. Available: https://www.bbc.com/news/world-europe-61327638

[60] J. G. Laura Navarro. (2022) After months of bombing, russia starts rebuilding mariupol. [Online]. Available: https://english.elpais.com/international/2023-01-13/after-months-of-bombing-russia-starts-rebuilding-mariupol.html

[61] N. Starkov. (2022) Russia drones smash power network in odesa. [Online]. Available: https://www.reuters.com/world/europe/russian-drone-attacks-target-power-network-ukraines-odesa-officials-2022-12-10/