Exploring Internet-Scale Data-Driven Intelligence: Empirical Analysis of the Russo-Ukrainian Conflict

Joseph Khoury*, Christelle Nader†, Morteza Safaei Pour‡ and Elias Bou-Harb*
* Division of Computer Science and Engineering, Louisiana State University, LA, USA
† Ernst & Young, TX, USA
‡ San Diego State University, CA, USA
Email: *jkhour5@lsu.edu, †christelle.nader@utsa.edu, ‡msafaeipour@sdsu.edu, *ebouharb@lsu.edu

2024 IEEE International Conference on Communications Workshops (ICC Workshops) | 979-8-3503-0405-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICCWORKSHOPS59551.2024.10615332

***Abstract*—In light of the numerous peculiar events that persistently challenge the world, it is paramount to possess the capacity to thoroughly analyze the realm of cyberspace and cyber threats in the context of these circumstances. As such, adequately integrating data-driven intelligence in cyber analytics can help strengthen security postures and enable effective decision making. In this paper, we introduce a multi-faceted Internet-scale, data-driven framework to enable the consistent measurement, identification and characterization of cyber threat dynamics amid real-world events. Particularly, our proposed framework scrutinizes Internet-wide security data feeds from multiple sources, including, *(i)* a large network telescope to infer illicit activities at large, *(ii)* a cluster of globally distributed sensor and honeypot to quantify reflective amplification attempts, and *(iii)* a set of BGP collectors to analyze Remotely Triggered Black Hole (RTBH) events. Specifically, we employ our framework to shed light on the 2022 Russo-Ukrainian cyber threat activities by drawing upon Terabytes of real network and security data feeds. We infer DDoS and UDP reflective attacks targeting federal agencies in Russia, and media entities in Ukraine. We further perceive an upsurge of Russian and Ukrainian RTBH techniques employed to block attacks targeting `.ru` domains and media companies. Additionally, we uncover an escalation of reconnaissance events, some of which are generated by the IoT-centric `Mirai` malware and others which target critical infrastructure. We report our findings objectively while postulating thoughts on intriguing observations on that particular event. Our Internet-scale data-driven framework offers a robust approach for empirical analysis of cyber threats in the face of real-world challenges; enabling effective and well-informed decision making.**

***Index Terms*—Internet-Scale Data-Driven Intelligence, Internet Measurements, Cyber threats, Network telescope, UDP honeypots, BGP routing data, Remotely Triggered Black Hole (RTBH) technique.**

I. Introduction

NATO leaders continue to attest cyberspace as a "*domain of military operations*" [1], where they have recently approved their new cyber-defense policy which aims at integrating and synchronizing cyber and kinetic capabilities in Multi-Domain Operations (MDO). This was a reaction to the repetitive use of methods which have been used by state-sponsored actors and others to disrupt and degrade networked information and communication systems. Cyberspace has been and will continue to be a major dimension of warfare, as evident during the ongoing 2022 Russo-Ukrainian conflict. Due to such strained conflict, a plethora of cyber threats have been publicly reported to target governments, commercial enterprises, Industrial control Systems (ICS), financial institutions, Internet Service Providers (ISP)s, and military command and control centers (e.g., [2], [3], and [4]).

While the literature has previously offered empirical measurements of state-sanctioned Internet outages and studies which explore threat dynamics, yet we perceive herein an opportunity to contribute to the operationalization of cyberspace (as described by NATO [1]) by proposing an innovative and a generic, data-driven cyber threat capability to measure, identify, and characterize cyber threat dynamics amid warfare-related events. In this vein, the objective of the proposed approach is to enable the near real-time generation and comprehension of threats, permitting, strategic and operational (mitigation) prioritization and decision making.

The proposed approach uniquely fuses and explores Internet-wide network traffic and routing data through the lens of multiple vantage points. These include *(i)* dark IP address spaces acting as a passive monitoring system to capture illicit Internet-wide network traffic; *(ii)* User Datagram Protocol (UDP) sensors for monitoring and tracking reflective amplification attempts; and *(iii)* route collectors to curate Border Gateway Protocol (BGP) updates associated with Remotely Triggered Black Hole (RTBH) techniques. Taking the ongoing 2022 Russo-Ukrainian conflict as an evolving case study, we employ our proposed approach to empirically shed light on the impact of such a crisis on the cyber threat landscape. Besides the novelty of our proposed approach in designing a streamlined pipeline by drawing-upon complementary and unique data feeds, we emphasize the promise of such an approach in supporting successive research efforts that aim to integrate and empirically analyze cyberspace to aid in kinetic operations.

We summarize the paper's contributions as follows:

- We devise a broadly-applicable approach that leverages three network security feeds including darknet, UDP sensor, and BGP routing data to measure, identify, and characterize cyber threat dynamics. This approach primarily aims at deriving threat intelligence amid warfare-related events to support MDO and steer strategic decisions.

Authorized licensed use limited to: Louisiana State University. Downloaded on December 23,2024 at 03:40:52 UTC from IEEE Xplore. Restrictions apply.

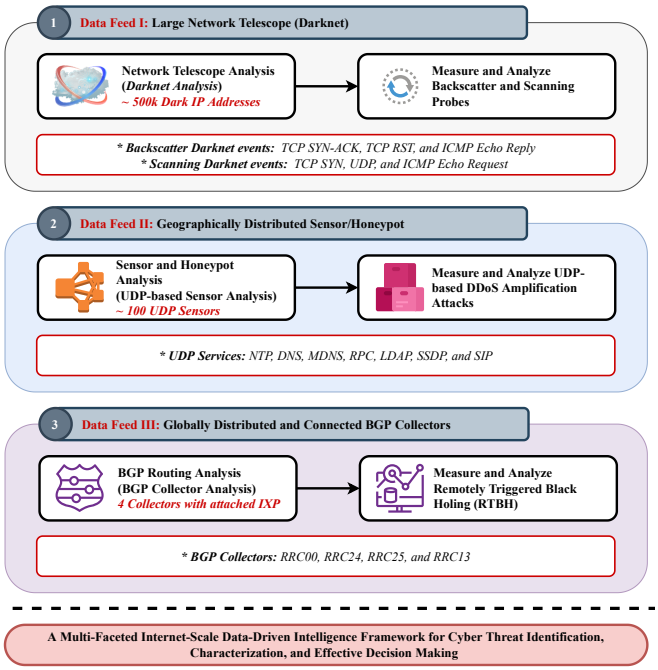

Fig. 1. The proposed empirically-driven pipeline that employs three different network security feeds to derive threat intelligence; enabling effective decision making.

- We demonstrate the merit of this approach by conducting an extensive 7-month measurement study from Dec. 1, 2021 to Jun. 30, 2022 to accentuate the devastating effect of the 2022 Russo-Ukrainian conflict on cyberspace.
- We automate the proposed pipeline to enable the reproducibility of the current work/results, while enabling successive research that aims at integrating and fusing tailored data (and security) feeds for effective threat intelligence which could provide vital situational awareness, especially amid volatile cyber-kinetic events.

The rest of the paper is as follows. The next section elaborates on the employed measurement methodology and related vantage points. Section III provides the analysis and results while postulating thoughts on key observations. Section IV presents the related work. Finally, Section V provides concluding remarks and future directions.

II. Vantage Points and Measuring Techniques

Herein, we thoroughly elaborate on our multi-faceted Internet-scale data-driven framework as illustrated in Figure 1.

Darknet Analysis. Primarily, we track, measure and analyze Internet-wide activities through the lens of a network telescope also referred to as a darknet. The darknet is a passive monitoring system consisting of dark IP address spaces that are routable, yet unused. Network traffic observed on the darknet is unidirectional and naturally illicit; there is no reason why hosts on the Internet should send packets to non-populated/active hosts. In this paper, we leverage Merit's ORION darknet [5], comprising 1856/24s subnets (i.e., around *500K* dark IPs) to identify and characterize malicious events. The ORION darknet continuously receives and records in real-time Terabytes of darknet packets in Packet Capture (PCAP) format. These packets are then processed and aggregated into darknet events based on the *source IP*, *destination port*, and *transport protocol fields*. These events are expired after a *627* seconds interval to ensure correct aggregation of events [6]. Two main types of events can be observed on the darknet, which include DDoS backscatters and malicious scanning probes. DDoS backscatter, also known as Internet background radiation, represent victims' replies to DDoS attacks with spoofed IPs that reach the darknet address space. Exploring such replies on the darknet permits the collection of various artifacts including, victim IP address, attack type and intent, as well as information on the duration and impact rate of the attack. Similarly, we identify from the darknet Internet-wide scanning probes originating from random and/or orchestrated scanning worms and botnets in the wild. Investigating these events typically reveal valuable intelligence on the probing source(s), the targeted port(s)/service(s), as well as the exact time, duration, and intensity of the probes. During warfare-related events, similar to the ongoing Russo-Ukrainian conflict, generating threat-related information pertained to backscatter and scanning events would offer valuable threat situational awareness as well as provide a strong indication of times of escalation and/or assets of interest (to be targeted/protected.)

To this end, we execute a longitudinal analysis over a 7-month period of darknet events by employing packet- and behavioral-based algorithms to extract backscatter and scanning events. These events are filtered using the packet transport protocol fields in which backscatter events are recognized by TCP SYN-ACK, TCP RST, and ICMP Echo replies packet fields, whereas scanning ones are identified with the TCP SYN, UDP, and ICMP Echo Request fields.

Sensor/Honeypot Analysis. As part of our proposed approach, we also aim to proactively analyze events targeting UDP reflectors (i.e., typically used in DDoS amplification attacks) by employing globally deployed sensor/honeypot nodes to uncover potential attacks and malignant intents surrounding hostile geopolitical events. Particularly, we leverage *100* globally distributed sensors deployed by the Hopscotch Sensor System (initially developed by the Cambridge Cybercrime Centre [7]). These sensors provision multiple UDP services including NTP, Domain Name System (DNS), Multicast DNS (MDNS), Remote Procedure Call (RPC), Lightweight Directory Access Protocol (LDAP), Simple Service Discovery Protocol (SSDP), and Session Initiation Protocol (SIP). In this context, we examine incoming traffic for protocol compliance, and if valid, a UDP packet is sent to the request's source IP. Notably, we respond to packets associated with scanning for reflectors that are often used in DDoS amplification attacks. We

Authorized licensed use limited to: Louisiana State University. Downloaded on December 23,2024 at 03:40:52 UTC from IEEE Xplore. Restrictions apply.

limit and cease the reflective packets when amplification attacks are detected to avoid assisting malicious actors in performing DDoS attacks [7]. Once the reflection is stopped, we employ a sniffer to record the details of the attack in a flat file format while including the flow information such as counts of packets from a given IP address to a particular port with the same arrival hop count (i.e., TTL field from the IP packet header), the victim IP address, the timestamp, the service port, and the number of packets. By drawing-upon such Internet-wide UDP sensors, we extend our observations in this paper to identify and characterize threat dynamics and trends targeting both Russia and Ukraine. Measuring such attacks provide insights on the number of targeted victims (and assets) in both countries, and yield unique understanding of attackers' behaviors and intentions amid such Russo-Ukrainian conflict.

RTBH Analysis. Border Gateway Protocol (BGP) is the de facto protocol for achieving global Internet reachability. BGP allows autonomously operated networks to share routing information with their local counterparts and, ultimately, with all Internet networks. Particularly, BGP exchanges `update` messages to advertise routing information. Remotely Triggered Black Hole (RTBH), a BGP technique, is an operational countermeasure that leverages the capabilities of BGP to mitigate various maliciousness, including DDoS attacks and spam as described in [8], [9]. RTBH routing is implemented using the BGP community attribute, a BGP extension that permits the transmission of additional information to BGP peers. In essence, it employs a specific set of BGP community tags to request an upstream provider ISP or Internet Exchange Provide (IXP) to drop (i.e., null route) traffic to a certain destination prefix. In this work, we complementary explore RTBH from large-scale BGP data; more specifically, blackholing community #666 due to the fact that most ASNs use this community number to initiate RTBH routing to drop traffic targeting a particular prefix [8]. RTBH routing has the potential to be prompt, inexpensive, and very effective, particularly when the attack volume is large that other mitigation techniques become impossible or costly. Thus, analyzing BGP updates associated with RTBH routing would provide very valuable information about the global victims of significant DDoS attacks. Herein, we leverage PyBGPStream from BGPStream [10], an open-source software framework which indexes and analyzes both historical and real-time BGP measurements. Our experimental setup and parameters can be found here [11]. By using streaming algorithms coupled with in-memory data structures, we efficiently explore this data by measuring and identifying any mitigation tactics and defensive measures used by Russia or Ukraine in an attempt to restrain or prevent targeted attacks. Between Dec. 2021, and Jun. 2022, we parse more than 100 GB of BGP updates gathered by four different route collectors. These include multi-hop collectors; RRC00, RRC24, RRC25 (globally-connected), and RRC13 (in Moscow with attached IXP peers).

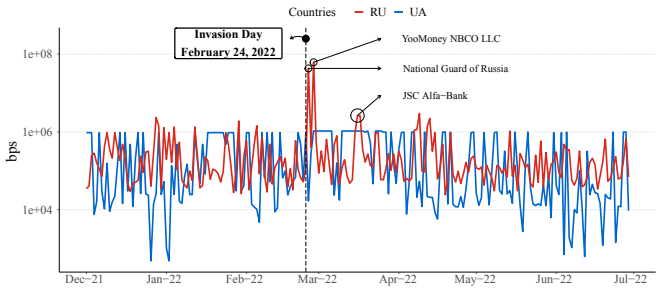

Fig. 2. A time series of DDoS rates (bps) for both Russia and Ukraine during the 7-month analysis period.

III. Measurements, Findings, and Discussions

In this section, we demonstrate and validate the capabilities of our approach by investigating and analyzing a 7-month duration spanning between Dec. 1, 2021, and Jun. 30, 2022. Please note that the devised approach is fully automated[1], instrumented by set of APIs, to extract threat-related information from the fused security feeds (i.e., *instructions:* [11]).

A. DDoS Backscatter and Scanning Probes

Darknet dynamics. By exploring around 2TB of darknet data, we filter and measure Internet-wide DDoS backscatters and scanning probes over the 7-month period. We break down the events by their appropriate traffic types to obtain a granular perspective on the impacted traffic and their dynamics with respect to the crisis under study. During our measurement, we observe a notable general increase in TCP SYN scanning events and TCP SYN-ACK backscatter events. Interestingly, the TCP SYN scanning events increased from *3.696* billion to *3.955* billion events between Feb. 2022 and Mar. 2022. Likewise, and during that same time period, TCP SYN-ACK DDoS backscatter events showed a significant increase from *83.564* million to *189.145* million events. This darknet perspective can distinctly exhibit how the 2022 Russo-Ukrainian crisis had in fact shaped the cyber threat dynamics at an Internet-wide level. As such, we dive more in the sequel into the analysis of the darknet data by investigating cyber threats linked to both conflicting countries.

DDoS attacks, rates, and targeted ports. To understand the illicit effect of the Russo-Ukrainian conflict on cyberspace, we measure and analyze different attacks targeting Russian and Ukrainian IP spaces. Figure 2 presents the maximum daily DDoS bits per second (bps) rates over the 7-month period for both Russia and Ukraine while showcasing selected notable attacks. For Russia, we observe various spikes throughout the different days of our measurement. However, just after the Russian invasion on Ukraine, we observe on Feb. 25, 2022, a significant

[1]Please reach out to the last author for access to the software.

Authorized licensed use limited to: Louisiana State University. Downloaded on December 23,2024 at 03:40:52 UTC from IEEE Xplore. Restrictions apply.

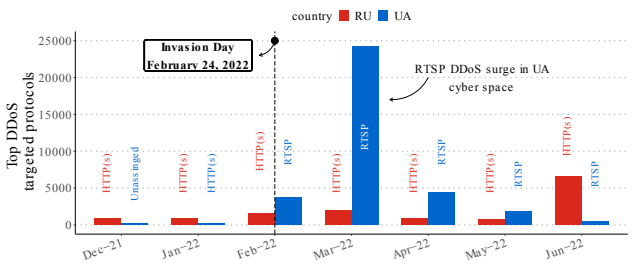

Fig. 3. Top DDoS targeted protocols in both Russian and Ukrainian Cyber Space during the 7-month analysis period.

DDoS attack of 4.3×10^7 bps targeting one of the major federal executive body, namely, "The National Guard of Russia". Additionally, we detect on Feb. 27, 2022, the largest DDoS attack comprising of 6.2×10^7 bps and targeting the second-largest electronic payment service in Russia, specifically, the "YooMoney NBCO LLC". Furthermore, a notable DDoS attack with a 2.6×10^6 bps is observed on Mar. 16, 2022 targeting the "JSC Alfa-Bank". On the other hand, within the Ukrainian IP space, we notice an overall lower DDoS rate compared to the Russian rates, mainly due to the overall lower number of IP addresses, hence the low number of observation on the darknet.

All things considered, the choice of the attacked victims, specifically, governmental and banking is a plain manifestation to the nefarious intention and objective of the aggressor in causing damage, chaos, and disorder in the cyberspace of both countries. In the same vein, it could be noted that such aggressors would be hacktivists, patriots, or state-sponsored groups belonging to both conflicting countries which are actively engaging in such activities. To further interpret the motives of the aggressors throughout this conflict, we retrieve the most DDoS targeted protocol(s)/port(s) in both Russian and Ukrainian IP spaces. Figure 3 presents these findings while showcasing their prevalence over the 7-month measurement. In Ukraine, we start to observe in Feb. 2022, and Mar. 2022, DDoS attacks targeting the previously unseen Real-Time Streaming Protocol (RTSP) with an occurrence of *3,770* and *24,235* attacks, respectively. RTSP continues to be the number one targeted protocol in Ukraine up until our last month of measurement. The RTSP protocol is primarily used in communication systems to control streaming media servers. This possibly reveals a malicious intent to disrupt media coverage with respect to the invasion. Additionally, in Russia, we observe a small surge of attacks targeting the HTTP(s) protocol (tcp/443) with a frequency of *1,543* in Feb. 2022 and *1,991* in Mar. 2022. As such, these attacks clearly reflect the intentions of the attackers in targeting media-related entities in Ukraine.

`Mirai`-based and ICS-related probes. Similar to the previous analysis, we parse and analyze a momentous volume of scanning events associated with both Russia and Ukraine. We primarily look into potential known signatures embedded in the scanning packets to uncover information related to the scanners, as well as the scanned ports to infer cyber threat intentions and behaviors. We note that most of the scanners were inferred to be using specific signatures as part of their scanning modules to avoid memory complications and to correctly validate responses to their scans.

During the Russo-Ukrainian conflict, we identify a significant number of scanning events associated with the prominent `Mirai` malware, an IoT-centric malware, taking a significant part in this conflict and prominently engaging in uncommon scanning activities. The `Mirai` malware is primarily identified by its signature where the destination IP in the TCP header is equal to the sequence number (i.e., *dst.IP = TCP.seq*). Additionally, we identify intriguing behaviors in scanning events targeting Industrial Control System (ICS) communication and control protocols. These scanning events are determined by corroborating the scanning destination ports with an extensive set of well-known ICS port(s)/protocol(s) [12]. We stress the fact that targeting ICS protocols during this conflict is concerning and mostly associated with reconnaissance-related activities to initially gather intelligence and subsequently attack critical infrastructure processes.

Figure 4 presents the number of `Mirai`-generated and ICS-targeted scanning events where both Russia and Ukraine are the sources. For Russian-based scanners, we observe on Feb. 13, 2022 an interesting surge of scans peaking at *111,644* unique events and mostly targeting the Telnet protocol. This behavior is also observed on May. 24, 2022 with a peak of *91,504*. Such spire of events is either a demonstration of Russian cyber-warfare capabilities in controlling a large botnet, such as `Mirai`, or an indication of large-scale violation and exploitation of IoT devices in the Russian IP space. Moreover, we observe between the very beginning of Feb. 2022 and the invasion day (`2` and `2′` on the graph) a deterioration followed by an increase in Russian scans towards ICS ports. Such activities are questionable and may indeed point to an intentionally restrained period of Russian ICS scans to deter attention, or contrarily, a period where Russian scanners started to employ decoy scanning techniques to hide their identities. For Ukraine, we observe an interesting spike of `Mirai`-related scans on Feb. 14, 2022, peaking at *17,732* unique events, and mostly targeting the Telnet protocol on port 2323 (`3` on the graph).

B. UDP-based Amplification Attacks

Herein, we aim to extend our exploration by performing a parallel 7-month measurement analysis using the UDP Hopscotch sensor system. In essence, we consider well-known UDP servers including NTP, DNS, MDNS, RPC, LDAP, SSDP, and SIP to measure UDP reflective attacks targeting Russian and Ukrainian victims amid the conflict. Figure 5 presents on the right y-axis the number of unique

Authorized licensed use limited to: Louisiana State University. Downloaded on December 23,2024 at 03:40:52 UTC from IEEE Xplore. Restrictions apply.

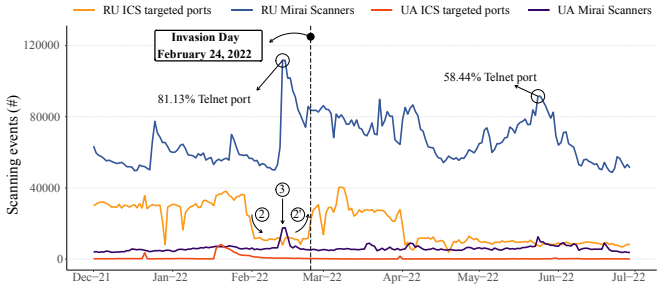

Fig. 4. The dynamics of scanning events originating from both Russian and Ukrainian IP spaces.

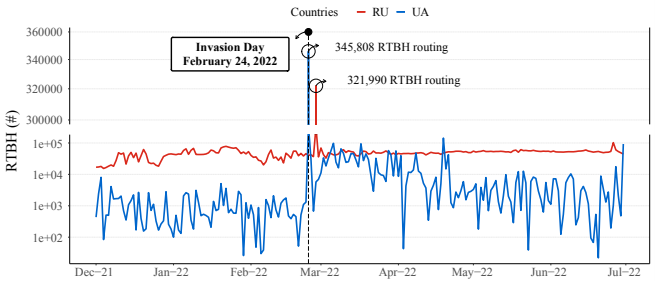

Fig. 6. The number of BGP updates, specifically RTBH routing associated with the top 5 ASNs belonging to both Russia and Ukraine.

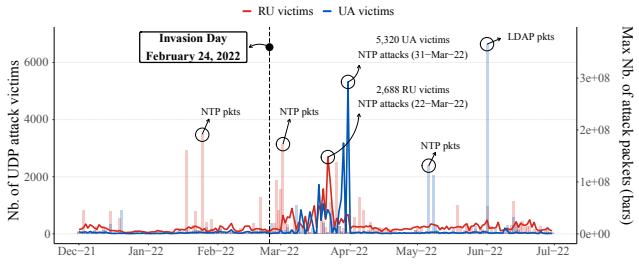

Fig. 5. The number of victims and maximum attack packets within the Russian (red/light red) and Ukrainian (blue/light blue) IP spaces targeted by reflective UDP amplification attacks.

victims and on the left y-axis the maximum number of attack packets (data presented as bars) associated with different UDP reflective attacks. We observe on Jan. 25 and Mar. 2, 2022 a buildup of NTP attacks targeting Two Russian telecommunication entities, namely, "Interra Telecom Group" and "ER-Telecom Holding", respectively. Additionally, within the Ukrainian IP space, we note on May. 6 NTP-related attacks and on Jun. 1, 2022 LDAP-related attacks targeting the "Private Enterprise Zharkov Mukola Mukolayovuch". Furthermore, on Mar. 22, 2022, we identify a huge leap of *2,688* Russian victims targeted by UDP reflective attacks, specifically *2,665* victims targeted by abusing the NTP service. Most of the targeted Russian IP addresses belongs to "National Guard of Russia", an observation that comes hand in hand with the DDoS attacks observed on the darknet. Although the attacks from the Hopscotch sensors are discovered at a different time, we consider this as an additional clue to the actual intention of the attackers in continuously targeting federal Russian agencies. Similarly, we perceive on Mar. 31, 2022, a significant peak of *5,320* Ukrainian victims out of which *5,306* targeted using NTP. Almost all of the detected Ukrainian victims are linked to IPs belonging to the "PP TRC city TV center" which associate quite well with the surge of RTSP DDoS attacks observed on Mar. 2022 via the darknet analysis.

C. BGP Updates and RTBH Routing

Using BGPStream and the four different route collectors (i.e., RRC00, RRC13, RRC24, RRC25), we measure RTBH null routing techniques used by Russian and Ukrainian ASNs over the 7-month measurement period. The aim is to assess the use of such mitigation tactics in restraining undesired traffic and DDoS attacks during the conflict. As previously discussed in Section II, we focus on BGP updates associated with the 666 blackholing community. Figure 6 presents the measurement results associated with RTBH routing originating from multiple Russian and Ukrainian ASNs. Specifically, we focus on the top five Russian ASNs (i.e., 31514, 49392, 8369, 51408, 49874), and the top five Ukrainian ASNs (i.e., 6849, 13188, 197481, 206777, 31148) which we observe having interesting dynamics in correspondence with the usage of the RTBH technique. On the invasion day, we note a huge increase of RTBH peaking at *345,808* RTBH routing out of which *345,015* originated from AS13188. Notably, most of the blackholed IPv4 and IPv6 prefixes belonged to "Triolan", a Digital Network and Cable Television in Kharkiv in Ukraine. A successive significant drop was observed on Feb. 26, 2022 in which we detected RTBH mostly associated with "Triolan" but with a much lower magnitude. Therefore, we postulate that "Triolan" might have been under attack during the first day of invasion and an automated defense mechanism associated with the RTBH technique was used to drop malicious traffic and/or that AS13188 was deliberately sending RTBH to proactively defend the various networks of "Triolan" against possible attacks. Recall, based on our findings in Figure 3, the RTSP protocol was increasingly targeted in Feb. 2022 with a significant volume of DDoS attacks. To this point, we postulate a direct connection between the RTSP-related DDoS attacks detected in our darknet analysis with the extensive use of RTBH routing by AS13188 detected in the BGP analysis.

Whereas in Russia, we perceive on Feb. 27, 2022 a rise of *321,990* RTBH out of which *282,419* originated from AS49392 associated with the "LLC Baxet company" which hosts multiple `.ru` websites. The web hosting nature of AS49392 clearly explains the excessive usage of RTBH to mitigate attacks targeting its hosted Russian domains.

IV. Related Work

The playground for the malicious cyber actors (e.g., state-sponsored, hacktivists, and others), namely, the Internet is immense, and constantly evolving. To achieve advanced

Authorized licensed use limited to: Louisiana State University. Downloaded on December 23,2024 at 03:40:52 UTC from IEEE Xplore. Restrictions apply.

cyber analytics for informed decision making, it is crucial to employ large vantage points across different verticals, covering the immense number of interconnected users, devices, and assets on the Internet. For instance, Antonakakis *et al.* [13] and Herwig *et al.* [14] have previously employed extensive security data feeds from distinct sources to study Internet-wide threats including the `Mirai` and `Hajime` botnet, respectively. Similarly, Khoury *et al.* [15] and others [16]–[19] have used the darknet as a security data source for detecting and analyzing illicit activities associated with in-the-wild cyber threats targeting various ecosystems. These ecosystems includes IoT devices, IoT-based Helium hotspots, Electrical Vehicles Charging Stations (EVCSes), and Low Earth Orbit (LEO) satellite terminals. In contrast to our analysis, which primarily focused on network-related attacks and Internet backbone routing activities, Hans *et al.* [20] studied information campaigns orchestrated by Russian state media outlets. They utilized a large-language model to perform sentence-level topic analysis on articles published in Russian websites. Furthermore, Anh *et al.* [21] delved into the role of the cybercrime underground community, employing different data sources from the Cambridge Cybercrime Centre and data from an online hacking discussion group. Their objective was to quantify the involvement of these entities in cyberwarfare. Nonetheless, our proposed multi-faceted framework distinguishes itself by amalgamating network security data feeds from different verticals to infer offensive, as well as defensive activities related to Internet-wide cyber threats. This approach enables us to closely examine the interplay between cyber threats and real-world challenges.

V. Concluding Remarks and Future Directions

In this work, we introduced a first-of-kind, automated empirical-driven pipeline by drawing upon a number of tailored, externally-sourced security data/network feeds to contribute to the operationalization of cyberspace. Considering the 2022 Russo-Ukrainian conflict, we demonstrated the merit and value of our proposed approach through disclosing related threat intelligence; by inferring key cyber threats targeting banking, federal, and telecommunication entities in Russia, as well as media protocols/entities in Ukraine, and other Internet backbone protocols. Indeed, promptly characterizing cyber threat dynamics amid real-world challenges posses a number of benefits, including the rapid comprehension of the situation and related landscape, for mitigation purposes as well as to support cyber-kinetic decision making processes. As such, we believe this work could possibly foster successive (empirical) research that aims at better integrating cyberspace in multi-domain operations. In our future work, we continue to aim at incorporating automated capabilities coupled with learning-based techniques to consolidate empirical artifacts (including machine-generated logs, malware dumps, network artifacts) with real-time defensive techniques to strengthen the security posture of critical national assets through insightful measurements and analysis.

References

[1] "Cyberspace domain of operations remains top priority for act," 2022. [Online]. Available: https://www.act.nato.int/articles/cyberspace-domain-operations-remains-top-priority-act

[2] L. Abrams, "New data-wiping malware used in destructive attacks on ukraine," 2022. [Online]. Available: https://www.bleepingcomputer.com/news/security/new-data-wiping-malware-used-in-destructive-attacks-on-ukraine/

[3] "Since february, 15, ukraine has suffered over 3000 ddos attacks," 2022. [Online]. Available: https://cip.gov.ua/en/news/vid-15-lyutogo-ukrayina-zaznala-ponad-3-000-ddos-atak

[4] "Ssscip ukraine's tweet," 2022. [Online]. Available: https://twitter.com/dsszzi/status/1513811072012140544

[5] "Orion network telescope," 2022. [Online]. Available: https://www.merit.edu/initiatives/orion-network-telescope/

[6] D. Moore, C. Shannon, G. M. Voelker, S. Savage *et al.*, *Network telescopes: Technical report*. Department of Computer Science and Engineering, University of California …, 2004.

[7] D. R. Thomas, R. Clayton, and A. R. Beresford, "1000 days of udp amplification ddos attacks," in *2017 APWG Symposium on electronic crime research (eCrime)*. IEEE, 2017, pp. 79–84.

[8] V. Giotsas, G. Smaragdakis, C. Dietzel, P. Richter, A. Feldmann, and A. Berger, "Inferring bgp blackholing activity in the internet," in *Proceedings of the 2017 Internet Measurement Conference*, 2017, pp. 1–14.

[9] "Blackhole community," 2016. [Online]. Available: https://www.rfc-editor.org/rfc/rfc7999

[10] C. Orsini, A. King, D. Giordano, V. Giotsas, and A. Dainotti, "Bgpstream: a software framework for live and historical bgp data analysis," in *Proceedings of the 2016 Internet Measurement Conference*, 2016, pp. 429–444.

[11] J. Khoury, "Ru-ua-measurement," 2023. [Online]. Available: https://github.com/josephKhoury95/RU-UA-measurement

[12] C. Fachkha, E. Bou-Harb, A. Keliris, N. D. Memon, and M. Ahamad, "Internet-scale probing of cps: Inference, characterization and orchestration analysis." in *NDSS*, 2017.

[13] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis *et al.*, "Understanding the mirai botnet," in *26th USENIX security symposium (USENIX Security 17)*, 2017, pp. 1093–1110.

[14] S. Herwig, K. Harvey, G. Hughey, R. Roberts, and D. Levin, "Measurement and analysis of hajime, a peer-to-peer iot botnet," in *Network and Distributed Systems Security (NDSS) Symposium*, 2019.

[15] J. Khoury, M. Safaei Pour, and E. Bou-Harb, "A near real-time scheme for collecting and analyzing iot malware artifacts at scale," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 2022, pp. 1–11.

[16] M. S. Pour, J. Khoury, and E. Bou-Harb, "Honeycomb: A darknet-centric proactive deception technique for curating iot malware forensic artifacts," in *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*. IEEE, 2022, pp. 1–9.

[17] V. Rammouz, J. Khoury, D. Klisura, M. S. Pour, M. S. Pour, C. Fachkha, and E. Bou-Harb, "Helium-based iot devices: Threat analysis and internet-scale exploitations," in *2023 19th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, 2023, pp. 206–211.

[18] K. Sarieddine, M. A. Sayed, C. Assi, R. Atallah, S. Torabi, J. Khoury, M. S. Pour, and E. Bou-Harb, "Ev charging infrastructure discovery to contextualize its deployment security," *IEEE Transactions on Network and Service Management*, 2023.

[19] N. Tieby, J. Khoury, and E. Bou-Harb, "Characterizing and analyzing leo satellite cyber landscape: A starlink case study," *IEEE ICC*, 2024.

[20] H. W. Hanley, D. Kumar, and Z. Durumeric, "Happenstance: utilizing semantic search to track russian state media narratives about the russo-ukrainian war on reddit," in *Proceedings of the international AAAI conference on web and social media*, vol. 17, 2023, pp. 327–338.

[21] A. Vu, D. Thomas, B. Collier, A. Hutchings, R. Clayton, and R. Anderson, "Getting bored of cyberwar: Exploring the role of low-level cybercrime actors in the russia-ukraine conflict," in *WWW The ACM Web Conference 2024*, 2024.

Authorized licensed use limited to: Louisiana State University. Downloaded on December 23,2024 at 03:40:52 UTC from IEEE Xplore. Restrictions apply.