An Internet-Scale Data-Driven Approach for Exploring Cyber Threats Amid Global Conflicts

Joseph Khoury, Christelle Nader, Morteza Safaei Pour, and Elias Bou-Harb

Abstract

The cyber domain demonstrates a profound interconnection with diverse global events, exerting its influence across social, political, and military realms. As a result, it is both rational and imperative to maintain a keen awareness of the threats that arise within the cyber domain. This can be achieved through robust cyber analytics and data-driven techniques to identify, analyze, and mitigate relevant cyber risks. As such, in this article, we elaborate on a unique, broadly-applicable, empirically-driven capability to enable the consistent measurement, identification and characterization of cyber threat dynamics. Specifically, we investigate and explore Internet-wide empirical data from diverse sources, namely, dark IP address spaces on the Internet to detect backscatter and scanning probes, globally distributed user datagram protocol (UDP) sensors to quantify reflective amplification attempts, and route collectors to ingest Border Gateway Protocol (BGP) routing data. As a case study, throughout an extensive 7-month measurement period, we employ the proposed approach to shed light on the 2022 Russo-Ukrainian cyber threat activities by drawing upon more than 150GB of real network and security data. 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 Remotely Triggered Black Hole (RTBH) techniques employed to block attacks targeting multiple Russian "`.ru`" country code top-level domain (ccTLD) 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 while postulating thoughts on intriguing observations.

Introduction

NATO leaders affirm cyberspace as a domain of military operations and have recently approved a new cyber-defense policy [1]. This policy integrates and synchronizes cyber and kinetic capabilities in Multi-Domain Operations (MDO) to counter state-sponsored actors disrupting networked systems. These disruptions create opportunities for adversaries to compromise critical national security assets. The ongoing 2022 Russo-Ukrainian conflict highlights the continued importance of cyberspace as a major dimension of warfare. Throughout this tense conflict, governments, commercial enterprises, industrial control systems, financial institutions, internet service providers, and military command and control centers have all faced targeted cyber threats. For example, Ukraine experienced ransomware attacks and distributed denial of service (DDoS) attacks, with one DDoS attack reaching a magnitude of almost 100Gbps [2]. Ukraine's largest ISP also suffered a near-total loss of connectivity due to a significant DDoS attack [3]. The Ukrainian energy sector was targeted by attacks linked to the Sandworm Advanced Persistent Threats (APT) [4]. Additionally, retaliatory DDoS attacks towards Russian IP addresses were discovered in a university campus network in the Czech Republic [5].

While the literature has previously offered empirical measurements of state-sanctioned Internet outages and studies which explore threat dynamics [6], yet we perceive herein an opportunity to contribute to the operationalization of cyberspace by proposing an innovative and a generic, data-driven cyber threat capability to measure, identify, and characterize cyber threat dynamics amid warfare-related events. These threats might include state-sponsored APTs, targeted DDoS attacks, and malware-related activities that could negatively impact core national security assets such as the communications, energy, and financial services' sectors. In this vein, the objective of the proposed approach is to enable the near real-time generation and comprehension of threats, permitting the technical, strategic and operational (mitigation) prioritization and decision making.

Given the limited research on network security data during global conflicts, we propose a novel approach that combines and analyzes Internet-wide network traffic and routing data through the lens of multiple vantage points. These include

- Dark IP address spaces acting as a passive monitoring system to capture illicit Internet-wide network traffic;
- User datagram protocol (UDP) sensors for monitoring and tracking reflective amplification attempts;

Joseph Khoury and Elias Bou-Harb are with Louisiana State University, USA; Christelle Nader is with Ernst & Young, USA; Morteza Safaei Pour is with San Diego State University, USA.

Digital Object Identifier: 10.1109/IOTM.001.2400044

2576-3180/24/$25.00 © 2024 IEEE

- Route collectors to curate Border Gateway Protocol (BGP) updates associated with Remotely Triggered Black Hole (RTBH) techniques. In this study, we use the ongoing 2022 Russo-Ukrainian conflict as a case study to highlight the potential of our proposed approach in examining the impact of the crisis on the cyber threat landscape.

We summarize the article's contributions and related derived insights as follows:

- We propose an empirical approach that utilizes three network security data feeds from different sources, including: (i) a large darknet, (ii) geographically distributed UDP sensors, and (iii) globally deployed BGP collectors. This approach aims to investigate cyber threats in the midst of global conflicts.
- We showcase the effectiveness of this approach by conducting a comprehensive 7-month measurement study spanning from Dec. 1, 2021 to Jun. 30, 2022. Using the darknet and the sensor/honeypot data, we infer DDoS and UDP reflective attacks targeting federal and banking agencies in Russia, media communication protocols and entities in Ukraine, and Internet backbone protocols in both countries. Additionally, we observe the escalation of the usage of the IoT Mirai malware and ICS-related scans originating from both Russian and Ukrainian IP spaces. In line with the observed attacks, we pinpoint a staggering increase in RTBH techniques during and after the invasion, originating from major Autonomous Systems (AS) in Russia and Ukraine, as a clear indicator of country-wide mitigation tactics against targeted attacks.

The rest of the article is as follows. The next section elaborates on the employed measurement methodology and related vantage points. We provide the analysis and results while postulating thoughts on key observations. Finally, we provide concluding remarks and future directions.

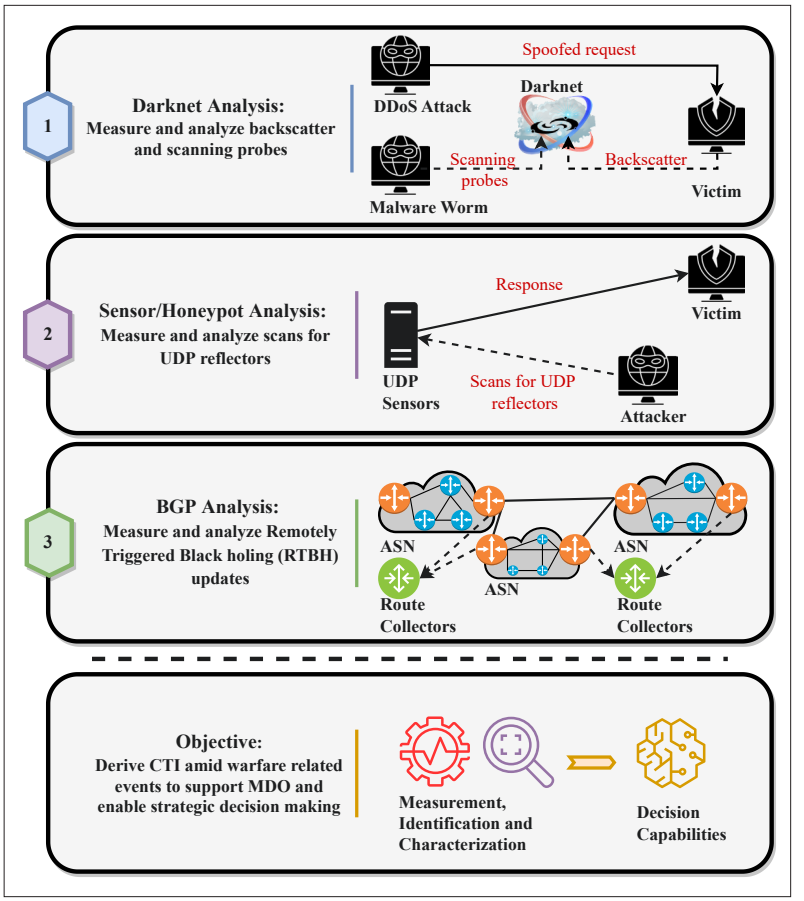

FIGURE 1. Proposed Empirical Approach: A multi-layered pipeline that utilizes three different network security data feeds to investigate cyber threats during global conflicts.

Vantage Points and Measuring Techniques

In this work, we propose a widely-applicable approach to measure, identify, and characterize cyber threats amid warfare-related events as illustrated in Fig. 1. Particularly, our approach uniquely combines three separate network security data feeds, enabling us to derive unprecedented Internet-wide malicious activities and insights specifically pertaining to global conflicts. Further details on the incorporated measurement techniques will be discussed in the sequel.

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 (e.g., malicious activities associated with IoT devices [7, 8]). In this article, we leverage Merit's ORION darknet [9], comprising 1856/24s subnets (i.e., 1856 subnets with a subnet mask of /24; around *500K* dark IPs) to identify and characterize malicious events. The ORION darknet captures and records darknet packets in real-time using Packet Capture (PCAP) format. These packets are processed and aggregated into darknet events based on *source IP*, *destination port*, and *transport protocol fields*. The darknet events primarily consist of DDoS backscatters and malicious scanning probes.

DDoS backscatter (i.e., recognized by TCP SYN-ACK, TCP RST, and ICMP Echo replies), 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 (i.e., recognized by TCP SYN, UDP, and ICMP Echo Request fields) 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).

Sensor/Honeypot Analysis. As part of our proposed approach, we also aim to proactively ana-

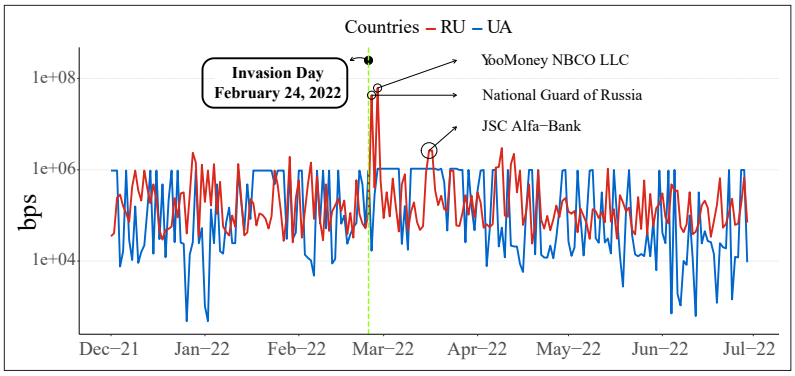

FIGURE 2. DDoS Rates (bps): A Comparative time series of DDoS rates for Russia and Ukraine over a 7-month analysis period.

lyze 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 [10]). 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 limit and cease the reflective packets when amplification attacks are detected to avoid assisting malicious actors in performing DDoS attacks [10]. 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 article to identify and characterize threat dynamics, trends, attackers' behaviors and intentions targeting both Russia and Ukraine.

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 [11, 12]. 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 [11]. 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 [13], 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 [14]. 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).

Measurements, Findings, and Discussion

Using our automated approach that extracts threat-related information from fused security feeds using APIs,[1] we study the 2022 Russo-Ukrainian conflict over a 7-month data period, analyzing cyber threat dynamics before and after the Russian invasion on February 24, 2022. The 3 months prior capture cyber trends, while the 4 months following reveal conflict-induced changes.

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,

[1] Researchers can use this approach during the same period for reproducibility or on different data time-frames for generating new insights related to other events of interest.

Country	Months	Top two Internet wide DDoS targeted protocols		ICS targeted protocols	
		Protocols (Port)	Freq.	Protocols (Port)	Freq.
Ukraine	December-2021	Unassigned (tcp/45464) Dynamic (tcp/60573)	223 216	ROC Plus (tcp/udp/4000) Telvent OASyS DNA (tcp/56048)	5,799 3,371
	January-2022	HTTP(s) (tcp/443)	136	ICCP (tcp/102)	61,114
		Unassigned (tcp/9508)	96	ROC Plus (tcp/udp/4000)	5,241
	February-2022	RTSP (tcp/554)	3,770	ICCP (tcp/102)	11,880
		HTTP(s) (tcp/443)	335	ROC Plus (tcp/udp/4000)	2,489
	March-2022	RTSP (tcp/554)	24,235	ROC Plus (tcp/udp/4000)	1,825
		BGP (tcp/179)	856	Telvent OASyS DNA (tcp/56048)	1,507
	April-2022	RTSP (tcp/554)	4,424	ROC Plus (tcp/udp/4000)	2,211
		HTTP(s) (tcp/443)	361	Foxboro DCS FoxApi (tcp/udp/55555)	32
	May-2022	RTSP (tcp/554)	1,818	ROC Plus (tcp/udp/4000)	2,618
		HTTP(s) (tcp/443)	664	Foxboro DCS FoxApi (tcp/udp/55555)	74
	June-2022	RTSP (tcp/554)	471	ROC Plus (tcp/udp/4000)	3,217
		HTTP(s) (tcp/80)	226	Foxboro DCS FoxApi (tcp/udp/55555)	116
Russia	December-2021	HTTP(s) (tcp/443)	872	ROC Plus (tcp/udp/4000)	121,918
		HTTP(s) (tcp/80)	603	Ethernet/IP (tcp/udp/448818)	68,166
	January-2022	HTTP(s) (tcp/443) HTTP(s) (tcp/80)	872 471	ROC Plus (tcp/udp/4000)	125,508
				ICCP (tcp/102)	68,401
	February-2022	HTTP(s) (tcp/443)	1,543	ROC Plus (tcp/udp/4000)	78,498
		HTTP(s) (tcp/80)	907	ICCP (tcp/102)	12,731
	March-2022	HTTP(s) (tcp/443) DNS (udp/53) and BGP (tcp/179)	1,991 1,823 and 1,258	ROC Plus (tcp/udp/4000)	108,254
				OMRON FINS (tcp/udp/9600)	40,831
	April-2022	HTTP(s) (tcp/443)	945	ROC Plus (tcp/udp/4000)	50,139
		HTTP(s) (tcp/80)	384	DNP/DNP3 (tcp/udp/19999)	7,657
	May-2022	HTTP(s) (tcp/443) HTTP(s) (tcp/80)	761 631	ROC Plus (tcp/udp/4000)	31,987
				DNP/DNP3 (tcp/udp/19999)	8,784
	June-2022	HTTP(s) (tcp/80) CWMP (tcp/udp/7547) and DNS (udp/53)	6,632	ROC Plus (tcp/udp/4000)	30,005
			4,033 and 2,257	DNP/DNP3 (tcp/udp/19999)	7,623

TABLE 1. Ports/Services Measurement: An overview of the top two most DDoS targeted and top two scanned ICS protocols. Protocols and frequencies are highlighted upon significant surges.

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 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. Part of Table 1 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

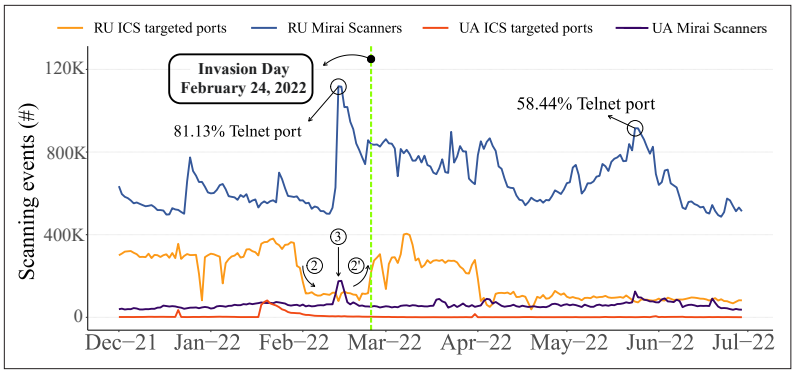

FIGURE 3. Scanning Events: The scanning dynamics of IoT Mirai scanners and targeted ports in ICS originating from Russian and Ukrainian IP spaces.

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 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. Moreover, we note in Mar. 2022 an unusual and concerning increase of DDoS attacks targeting Internet backbone protocols, including the DNS and BGP protocols in both countries. Interestingly, in Jun. 2022, we observe a buildup of attacks targeting the HTTP(s), DNS, and the CPE Wan Management Protocol (CWMP) protocols. That being said, these attacks indeed reflect the intentions of the attackers in targeting media-related entities in Ukraine and disrupt normal Internet operations in both countries.

Mirai-based and ICS-related probes. Similar to the previous analysis, we parse and analyze a momentous volume of scanning events from Russia and Ukraine, focusing on known signatures to uncover information about the scanners and infer cyber threat intentions and behaviors. 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) [15]. 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 3 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. These activities raise questions about intentional restraint or the use of decoy scanning techniques by Russian scanners to conceal 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). Furthermore, we investigate ICS targeted protocols to infer possible attack behaviors and intents linked to specific critical infrastructure during the conflict. Part of Table 1 presents the top two scanned ICS ports during the 7-month period. Interestingly, we observe in Jan. and Feb. 2022, significant scanning probes originating from both Russia and Ukraine and targeting the ICCP protocol, which is typically used to facilitate data exchange between Energy Management Systems (EMS) and Supervisory Control and Data Acquisition (SCADA) systems. Moreover, we identify, throughout our measurement, scans from Russia targeting the ROC Plus, OMRON FINS, and the DNP/DNP3 protocols which are used to facilitate communication among critical devices in various industries including the oil and gas sectors.

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 4 presents on the right y-axis the number of unique 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-to-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.

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, we focus on BGP updates associated with the 666 blackholing community. Figure 5 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 Table 1, 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 Russian "`.ru`" country code top-level domain (ccTLD). The web hosting nature of AS49392 clearly explains the excessive usage of RTBH to mitigate attacks targeting its hosted Russian domains.

Concluding Remarks and Future Directions

In this article, we presented an automated empirical-driven pipeline in which we employed tailored security data/network feeds to operationalize cyberspace. As a case study rendered by the 2022 Russo-Ukrainian conflict, we demonstrated the value of our approach by uncovering related threat intelligence, including cyber threats targeting various entities in Russia and Ukraine. Rapidly understanding cyber threat dynamics during geopolitical conflicts offers benefits for situation comprehension, mitigation, and supporting cyber-kinetic decision-making processes. Our future endeavors will focus on the integration of supplementary security data feeds, as well as refining the proposed empirical approach, to empower comprehensive decision-making amidst global conflicts.

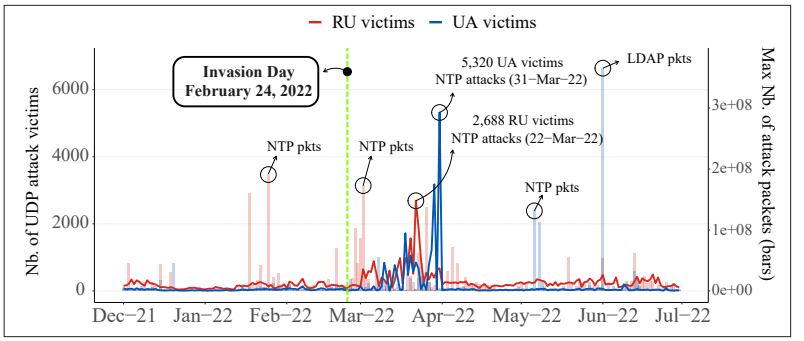

FIGURE 4. UDP Amplification Victims: The number of victims and maximum attack packets targeted by reflective UDP amplification attacks within the Russian (red/light red) and Ukrainian (blue/light blue) IP spaces.

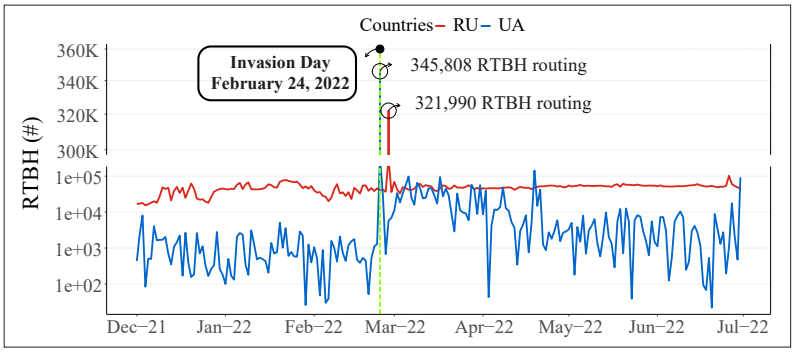

FIGURE 5. RTBH Measurement: The number of RTBH routing originating from the top five Russian and Ukrainian ASs.

References

[1] NATO, "Cyberspace Domain of Operations Remains Top Priority for ACT;" https://www.act.nato.int/articles/cyberspace-domainoperations-remains-top-priority-act, 2022.

[2] CIP, "Since February, 15, Ukraine Has Suffered Over 3000 DDoS Attacks;" https://cip.gov.ua/en/news/vid-15-lyutogo-ukrayina-zaznalaponad-3-000-ddos-atak, 2022.

[3] Forbes, "The Cybersecurity Risk No One Talks About—Until It's Too Late;" https://www.forbes.com/sites/thomasbrewster/2022/03/28/hugecyberattack-on-ukrtelecom-biggest-since-russian-invasion-crashesukraine-telecom/?sh=49490fab7dc2, 2022.

[4] SSSCIP Ukraine, "SSSCIP Ukraine's Tweet," https://twitter.com/dsszzi/status/1513811072012140544 , 2022.

[5] M. Husák, M. Laštovička, and T. Plesník, "Handling Internet Activism During the Russian Invasion of Ukraine: A Campus Network Perspective," *Digital Threats: Research and Practice*, 2022.

[6] G. Aceto *et al.*, "A Comprehensive Survey on Internet Outages," *J. Network and Computer Applications*, vol. 113, 2018, pp. 36–63.

[7] J. Khoury, M. Safaei Pour, and E. Bou-Harb, "A Near Real-Time Scheme for Collecting and Analyzing Iot Malware Artifacts at Scale," *Proc. 17th Int'l. Conf. Availability, Reliability and Security*, 2022, pp. 1–11.

[8] M. S. Pour, J. Khoury, and E. Bou-Harb, "Honeycomb: A Darknetcentric Proactive Deception Technique for Curating IoT Malware Forensic Artifacts," *NOMS 2022–2022 IEEE/IFIP Network Operations and Management Symp*, 2022, pp. 1–9.

[9] MERIT, "ORION Network Telescope," https://www.merit.edu/initiatives/orion-network-telescope/, 2022.

[10] D. R. Thomas, R. Clayton, and A. R. Beresford, "1000 Days of UDP Amplification DDoS Attacks," *2017 APWG Symp. Electronic Crime Research (eCrime)*, 2017, pp. 79–84.

[11] V. Giotsas *et al.*, "Inferring BGP Blackholing Activity in the Internet," *Proc. 2017 Internet Measurement Conf.*, 2017, pp. 1–14.

[12] rfc-editor, "BLACKHOLE Community;" https://www.rfceditor.org/rfc/rfc7999, 2016.

[13] C. Orsini *et al.*, "Bgpstream: A Software Framework for Live and Historical Bgp Data Analysis," *Proc. 2016 Internet Measurement Conf.*, 2016, pp. 429–44.

[14] Joseph Khoury, "RU-UA-Measurement;" https://github.com/josephKhoury95/RU-UA-measurement, 2024.

[15] C. Fachkha *et al.*, "Internet-Scale Probing of CPS: Inference, Characterization and Orchestration Analysis," *NDSS*, 2017.

Biographies

Joseph Khoury is a Ph.D. candidate in Computer Science and Engineering specializing in Cybersecurity at Louisiana State University (LSU). He holds a Bachelor's degree from the Holy Spirit University of Kaslik (USEK) and a Master's degree from the American University of Beirut (AUB), both in Computer Science. His research and development focuses on several areas: (i) Internet-scale measurements (both passive and active) to detect malicious cyber activities; (ii) applying advanced machine learning techniques such as Temporal Graph Neural Networks (TGNNs) to identify Advanced Persistent Threats (APTs) tactics at the network level; (iii) using Large Language Models (LLMs) to detect and repair software vulnerabilities in source and binary code; and (iv) developing cyber defense training materials for cyber forces.

Christelle Nader is a cybersecurity consultant at Ernst & Young who graduated, in 2022, with an M.S. in Information Technology at the University of Texas at San Antonio with a concentration in cybersecurity. Her research interests include operational cyber security, IoT security, attack detection and characterization, malware analysis, data science, Internet measurements for cyber security, and big data analytics.

Morteza Safaei Pour is an Assistant Professor in the Management Information Systems Department at San Diego State University. He earned his Ph.D. in Information Technology and Cyber Security from the University of Texas at San Antonio. His research encompasses operational cyber security, Internet measurement, artificial intelligence, and decision support systems.

Elias Bou-Harb [SM] received his postdoctoral training at Carnegie Mellon University and his Ph.D. degree in computer science from Concordia University, Montreal, Canada. He is currently an associate professor with the department of computer science at Louisiana State University, specializing in cyber security and data science as applicable to national security challenges. Previously, he acted as the director of the cyber center for security and analytics at the University of Texas at San Antonio, where he led and organized university-wide cyber security research, development, and training initiatives. He has authored more than 150 refereed publications in leading venues and has acquired significant state and federal cyber security research grants. His research and development activities focus on operational cyber security, cyber forensics, critical infrastructure security, empirical data analytics, digital investigations, network security, and network management. He is the recipient of five best research paper awards, including the ACM's best digital forensics research paper.