Journal of Advances in Mathematical & Computational Sciences
An International Pan-African Multidisciplinary Journal of the SMART Research Group
International Centre for IT & Development (ICITD) USA
© Creative Research Publishers
Available online at https://www.isteams.net/ mathematics-computationaljournal.info
DOI: dx.doi.org/10.22624/AIMS/MATHS/V9N1P2
CrossREF Member Listing - https://www.crossref.org/06members/50go-live.html

Dyn DDoS Cyberattack: A Position Paper

Ademola, E.O.
Professor, BCS & CMI Subject Matter Expert
Principal Consultant
Power-Age Consulting
E-mails: ojo_ademola@hotmail.co.uk (private); emmanuelojoademola.academia.edu
Mobile: +4479 5813 9157

ABSTRACT

The strategy adopted in the Dyn distributed denial of service (DDoS) attack remains a purported accentuation to classify it as a recent state-of-the-art DDoS even though it took place in 2016. It was one of the biggest DDoS ever launched and affected the availability of essential internet services. In exploiting vulnerabilities, the attack exposed the insecurity that surrounds some IoT devices. It helps experts in further deployment of detection techniques and countermeasures strategy. In this paper, a multi-stakeholder approach to mitigating against such attacks explored by critically analyse and reflect on the Dyn DDoS attack and hacking techniques. A discussion on possible countermeasures followed to suggest hybrid solutions by multiple different organisations to provide a secured solution to the internet against similar attacks.

Keywords — Countermeasures, vulnerabilities, DDoS, IoT, Cyber Security

Oyemade, D.A. & Allenotor, D. (2021): Dyn DDoS Cyberattack: A Position Paper. Journal of Advances in Mathematical & Computational Science. Vol. 9, No. 1. Pp 13-20. DOI: dx.doi.org/10.22624/AIMS/MATHS/V9N1P1. Available online at www.isteams.net/mathematics-computationaljournal.

1. INTRODUCTION

The Dyn assault, which occurred on 21st October of 2016, is one of the most significant information ruptures ever. The attack toppled an expansive bit of the web in the United States and Europe and influenced a lot of administrations. The wellspring of the assault was the Mirai botnet. It is an abnormal botnet for different reasons, comprising of purported Internet-of-Things (IoT) gadgets (Booth and Andersson 2016), for example, internet protocol (IP) and related conventions, cameras, printers, digital video recorders. All devices connected and applicable in smart-homes and other similar designs of smart cities. Dyn is an Internet Performance Management (IPM) organisation, reputably considered as a pioneer domain name system (DNS) specialist co-op. They additionally offer web foundation administrations and items, for example, observing and examination, control, online framework improvement and email.

Dyn escalates the art of DNS provision both by design and default (Liu et al., 2018; see also Booth and Andersson 2016; Wang et al., 2016). The goal of a Denial of Service (DoS) assault is to deny or upset approved clients from getting to an asset or administration. It is a fundamental attack on the availability of resources as the final leg of the CIA triad. For this malignant movement, the aggressor utilises one bot to flood the focused on injured individual or asset denying access to the approved clients. On account of Distributed Denial of Service (DDoS) assault a great many bots are controlled by the assailant to flood the focused on the unfortunate casualty. The sources from Dyn announced that the specialist co-op encountered a DDoS assault, which thrown numerous challenges in the form of the necessity of a suitable cyber defence mechanism (Kumar and Pandey 2016).

Further, the features of network traffic and the existing algorithms to detect DDoS could be an issue. In addition to several propositions for efficient detection, David and Thomas (2019) recently proposed a mechanism, which underpins a statistical approach to detect DDoS attacks based on traffic features and dynamic threshold detection algorithm. Indicatively, alleviating DDoS assaults was regular to the Network Operations Center (NOC) group of Dyn. Notwithstanding, the NOC group could distinguish that this assault was strange and peculiar. This work underscores Dyn DDoS as a recent state-of-the-art attack; excavating understanding of DDoS attacks and hacking mechanism with a brief reflection using more than twenty sources between 2015 to date.

2. CYBERATTACK CONCEPT- DDOS

Researchers over the years have taken DDoS attacks as hacking technique seeking to bring down a site, application, or foundation by flooding it with requests (Rebecchi et al. 2017; see also Liu et al. 2018 and Ramanathan et al. 2018). However, the foundational element of much of this activity, and the growth of attack, which saw around 2 8 million assaults in the central portion of 2018; as well as innovative strategy of attack in surveys considered as its pervasiveness (Haque et al. 2019; see also Rai et al. 2019 and Wang et al. 2016).

Moreover, with DDoS peak sizes skyrocketed, as the Memcached-based attacks that started in February 2018 ushered in the terabit era of attacks, the scope widens appropriately. With the size of attacks increment to 47 assaults more than 300 Gbps in the primary portion of 2018, contrasted and 7 in a similar timespan of 2017 DDoS crimes have never been progressively creative, dynamic, or significant, and there could be much increasingly risky DDoS assaults not too far off. Further, the dimension to DDoS, as well as the detection techniques (DT) and countermeasures strategies (CS) sufficing due to research, the scope keep upping.

Apparently, Rebecchi et al. (2017) based detection technique on the advanced in-switch processing capabilities to delegate traffic monitoring and DDoS detection using stateful SDN. What of the Learning Automata-based DDoS Attack Defense Mechanism in Software Defined Networks (Sahoo et al. 2018)? Nonetheless, DDoS geometrically gaining traction within its taxonomy in Figure 1, volume sizes and trend via infographic in Figure 2.

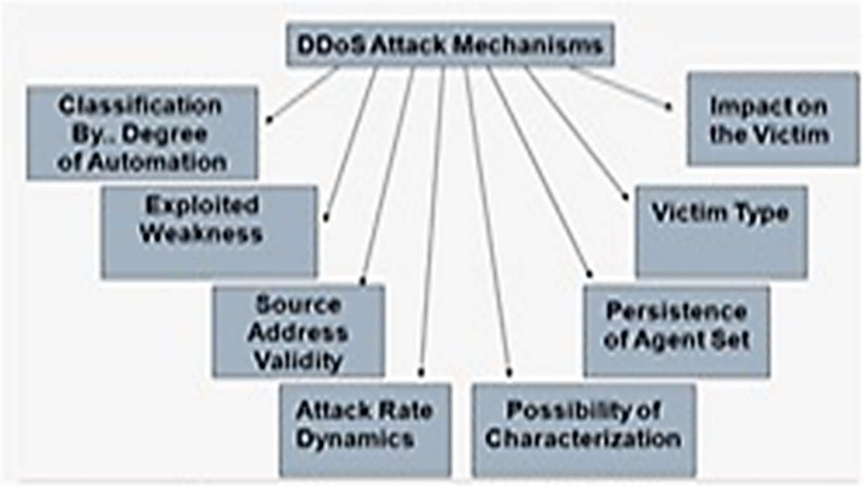

Fig. 1: Taxonomy of DDoS Attacks

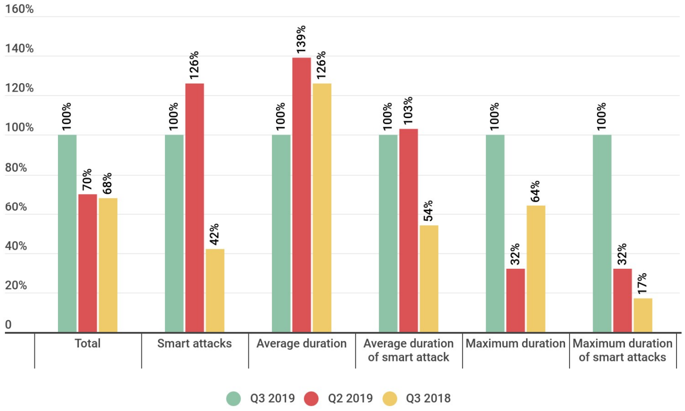

Fig. 2: Infographics for Volumes and Trends; Adapted from: DDoS report Q3 2019 | Securelist

3 THE THRUST OF THIS PAPER

This examination is on the literature concerned with the Dyn DDoS attacks as a position paper. Therefore, other studies that have considered the DDoS attacks over different areas (i.e. education, social, political, and management) at this moment excluded. What's more, this examination was additionally limited to articles with impact factor written in the English language. In various words, the materials therein referenced as expected in a reputable journal, having enough record. It guarantees specialists notes as surveyed by a few different researchers in the field to protect the paper's quality. DDoS attacks and related issues represent an attractive area of interest for both researchers and practitioners (Lun et al. 2019). Indeed, there exist several studies that have examined the relevant aspects of DDoS attacks with various academic themes and explications.

Nonetheless, less consideration has been paid to look at a multi-stakeholder approach to resolve the issues raised in Dyn DDoS attacks from the information security management perspective as mentioned in Sampigethaya et al. (2018); and Shackelford and Brady (2017). By doing so, not more than twenty articles collected that covered between 2015 up-till-to-date. These articles are in different interests, and themes. They are listed on the references as essential to this paper.

3.1 Background and Motivation

The history of DDoS since the inception comes with several practical implementations and views on mitigating the attack. For instance, considering the model of DDoS attack and related mechanism in Figure 3, Figure 4 respectively. It is apparent that discussion of detection mechanism (DT) and countermeasure strategy (CS) take a central stage. By analysis, some peer-reviewed articles on the DDoS, traction of DT and CS keep raising; as research ranges severally. Nowadays, Soft Computing or Artificial Intelligence-based methods are applied extensively for the attack detection (Singh et al. 2015). Based on analysis methods, detection approaches classified into Signature-based, Anomaly-based and Hybrid detection (Kaur et. 2017).

The emerging trend of IoT and DDoS capable IoT Malware, also aggravate the DT and CS emergent. For instance, De Donno et al. (2017) propose that a large portion of the innovation in the market today are either seriously structured or don't include security esteem as the IoT gadgets security becomes more terrible than any time in recent memory by permanently patching up old DDoS assaults. The various DT and CS model around could tally variously.

Further, algorithmic approach to DT and CS could improve the quality of service (QoS) via a multi-layer dynamic (Yan et al. 2018) as well developing the preventive solutions against DDoS (Somani et al. 2017; see also Bawany et al. 2017, Haddadi and Beghdad 2018). Such an approach could lead to hybrid techniques (Girma and Wang 2018) with the use of the DNS timer design changes algorithms (Booth and Anderson 2017). The outcome of completing a data mining approach (Tama and Rhee 2015) with a Clustered and or filtered-based defence mechanism (Keerthika et al. 2017; Shameli-Sendi et al. 2015) against DDoS could scale up the frameworks arguably.

Nonetheless, the statistical model to explicate threat modelling could provide a broader platform for professional engagement in mitigating against DDoS attacks (Saif et al. 2018). In an approach to augment the characterisation factors with the analysis of previous attacks, it could be a delving into the internet to suffice DDoS attacks by botnets in specifying IoT vulnerabilities (Wang et al. 2018). In all this, ethical questions cut-across both professional and academic discussions about DT and CS against DDoS.

The synergy of national, bilateral and or global CS strategy considering information governance and policy approach are all engaging. Summative, it could be a justification that if devices connected via the internet add values to various activities of human endeavour, the issue of security should also be integrated to provide the multi-stakeholders approach to mitigating the DDoS Attacks and the related impact; a viewpoint expressed in this paper.

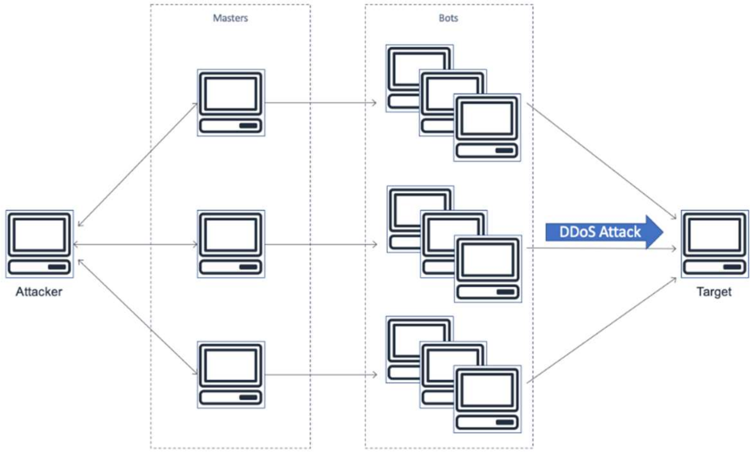

Fig. 3: Model of DDoS; Adapted from: Introduction: Denial of Service Attacks

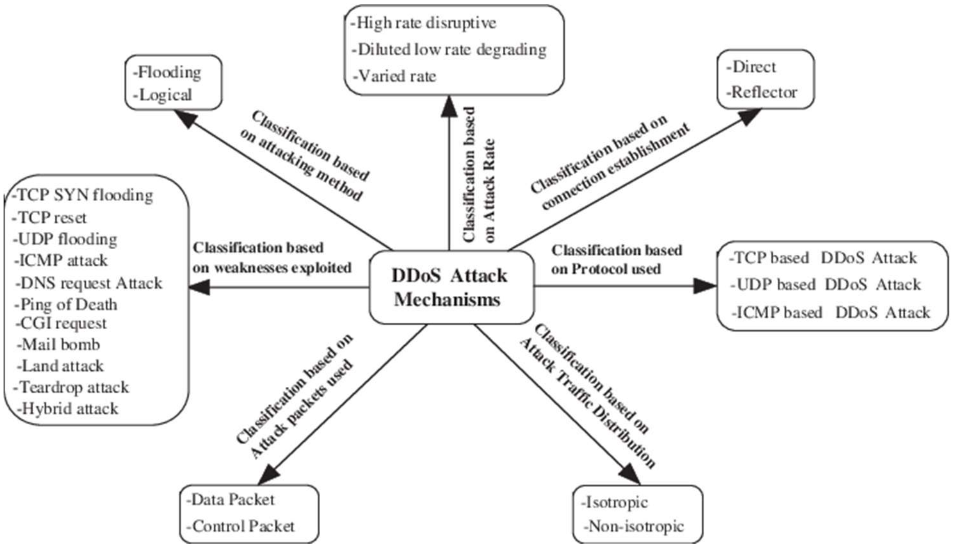

Fig. 4: DDoS Attack Mechanism
Adapted from: Classification of DDoS attack Mechanisms

4. ANALYSIS OF EFFECT-TREND

Dyn server was the target of this DDoS assault, and it influenced anycast servers. It likewise kept the administrations for settling genuine DNS questions (Liu et al. 2018). It is assessed to have created more than 40 to multiple times of the normal traffic volume and the typical number of included botnets amid the assault adds up to 100,000 (De Donno et al. 2017; see also Hilton 2016 and Krebs 2016). Per a couple of reports, analytically, the complete volume of information required amid this assault is evaluated to be 1.2Tbps. A couple of significant US sites including Paypal, Spotify, Twitter and Amazon confronted availability issues.

The different other web administrations of organisations, like HSBC, BankWest and Ticketmaster, additionally impacted (Mansfield-Devine 2016). Weagle (2017) notes that the financial impact enormous as well as trust eroded. Roughly 8% of the Dyn DNS client base ended their agreement after the assault. In addition to economic, ethical and security culture impacts, consequently, Kolias et al. (2017) correlate the lessons learned from Dyn DDoS attack to the risks associated with IoT devices pose to the Internet. Indeed, even credulous methodologies can pick up control of such gadgets and make a vast and exceedingly problematic of zombie gadgets. The simplicity of contamination and steadiness of the produced bot populace are appealing elements for any aggressor. An impact that calls for an integrated approach to solutions envisioned.

5.1 Multi-Stakeholder Mitigation Actions

The various DT and CS underscored in section 4.0 provide three spread-of-mitigation by design. Actions that a single defender can initiate and execute to defend against a DDoS attack, efforts to secure the interconnectedness of the IoT devices, and activities on a global level to minimise such attacks. The singular defensive CS of awareness, undoubtedly on the increase to sensitise individuals, organisations and governments about the existence and proliferation impact of DDoS attacks (Mansfield-Devine 2017; Weagle 2017). The daily broadcasts become an ever awareness platform for such mitigation as well as various lessons learned.

The emergent of IoT devices: DDoS-capability of such devices, envisioning various DT and CS claims, indeed could be a singular or compound approach to mitigating DDoS attacks of Dyn dynamic. Dyn DDoS was not new, but the proliferation of IoT devices and applications added new dimensions for both scholar-professional approaches to alleviating it. The accentuation of this paper should not be view as a counterclaim, but a lateral claim for multi-stakeholder governance approach bringing designs to mitigate DDoS attack globally! The most technical approach, as well as the information governance, could provide a hybrid dynamic to such solution approach. Specifying a global alleviation could be a test just as plan a half and a half to get the job done a multi-partner could recognise a variation of the web spine administrators. It could cut from the framework before they even achieve the goal. The IoT gadgets itself could proactively anchor against these assaults with a utilisation randomised default password to produce a significant effect. The lessons learned so far could lead to such global synergy (Ho 2018; see also Kolias et al. 2017 and Wirth 2017).

5. CONCLUSION

Undoubtedly, the Dyn DDoS attack did not consist of any mechanisms that were ground-breaking in their nature. All the tools were popular and manageable. However, what was new was the way the Mirai worm joined different assaults into one and contaminated a considerable number of uncertain gadgets. This massive volume of the distributed attack could be strange. Considering the escalating number of DDoS attacks, mitigating them could prove fundamentally challenging; in addition to the immense amount of source machines. Crossover arrangements are vital from various partners extending from spine suppliers to administrators to gadget makers. In this manner, until noteworthy changes in how the web is set up and controlled occur, specialist co-ops can't rely on the issue being fixed all things considered. Instead, to get ready for these assaults each administration head needs a top to bottom barrier procedure, adjusting to their very own necessities. Conclusively, such scope and limited resource could provide an incentive for the claim for a hybrid multi-stakeholder governance approach to delivering a secured solution to the internet against DDoS attacks, the countermeasure against capable IoT Malware devices and related cyberattacks.

REFERENCES

1. Bawany, N.Z., Shamsi, J.A. and Salah, K., 2017. DDoS attack detection and mitigation using SDN: methods, practices, and solutions. *Arabian Journal for Science and Engineering*, *42*(2), pp.425-441.
2. Booth, T. and Andersson, K., 2017, August. DNS DDoS Mitigation, via DNS Timer Design Changes. In *International Conference on Future Network Systems and Security* (pp. 43-55). Springer, Cham.
3. Booth, T. and Andersson, K., 2016, November. Network DDoS Layer 3/4/7 mitigation via dynamic web redirection. In *International Conference on Future Network Systems and Security* (pp. 111-125). Springer,.
4. David, J. and Thomas, C., 2019. Efficient DDoS Flood Attack Detection using Dynamic Thresholding on Flow-Based Network Traffic. *Computers & Security*.
5. De Donno, M., Dragoni, N., Giaretta, A. and Spognardi, A., 2017, September. Analysis of DDoS-capable IoT malwares. In *Computer Science and Information Systems (FedCSIS), 2017 Federated Conference on* (pp. 807-816). IEEE.
6. Girma, A. and Wang, P., 2018. AN EFFICIENT HYBRID MODEL FOR DETECTING DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS IN CLOUD COMPUTING USING MULTIVARIATE
7. Haddadi, M. and Beghdad, R., 2018. DoS-DDoS: TAXONOMIES OF ATTACKS, COUNTERMEASURES, AND WELL-KNOWN DEFENSE MECHANISMS IN CLOUD ENVIRONMENT. *EDPACS*, *57*(5), pp.1-26.
8. Haque, M.R., Tan, S.C., Yusoff, Z., Lee, C.K. and Kaspin, R., 2019. DDoS Attack Monitoring using Smart Controller Placement in Software Defined Networking Architecture. In *Computational Science and Technology* (pp. 195-203). Springer, Singapore.
9. Hilton, S., 2016. Dyn analysis summary of Friday October 21 attack. *Dyn Blog, Oct*.
10. Ho, A.M., 2018. Unlocking ideas: Using escape room puzzles in a cryptography classroom. *PRIMUS*, Kaur, P., Kumar, M. and Bhandari, A., 2017. A review of detection approaches for distributed denial of service attacks. *Systems Science & Control Engineering*, *5*(1), pp.301-320.
11. Keerthika, M.R., Nalini, C., Suganthi, M.P. and Abinaya, M.S., 2017. Cluster Based DDoS Detection Method in Data Mining. *International Journal Of Engineering And Computer Science*, *6*(3).
12. Kolias, C., Kambourakis, G., Stavrou, A. and Voas, J., 2017. DDoS in the IoT: Mirai and other botnets. *Computer*, *50*(7), pp.80-84.
13. Krebs, B., 2016. Did the Mirai botnet really take Liberia offline. *Krebs on Security*, *4*.
14. Kumar, U. and Pandey, S.K., 2016, August. Dynamic Model on DDoS Attack in Computer Network. In *Proceedings of the International Conference on Informatics and Analytics* (p. 11). ACM.

15. Liu, Y., Wang, Z. and Li, N., 2018, February. Characterizing the Impact of DDoS Attack on Inter-domain Routing System: A Case Study of the Dyn Cyberattack. In *2018 International Conference on Computer Science, Electronics and Communication Engineering (CSECE 2018)*. Atlantis Press.
16. Lun, Y.Z., D'Innocenzo, A., Smarra, F., Malavolta, I. and Di Benedetto, M.D., 2019. State of the art of cyber-physical systems security: An automatic control perspective. *Journal of Sys and Software*, *149*, pp.174-216.
17. Mansfield-Devine, S., 2016. DDoS goes mainstream: how headline-grabbing attacks could make this threat an organisation's biggest nightmare. *Network Security*, *2016*(11), pp.7-13.
18. Rai, S., Sharma, K. and Dhakal, D., 2019. A Survey on Detection and Mitigation of Distributed Denial-of-Service Attack in Named Data Networking. In *Advances in Communication, Cloud, and Big Data* (pp. 163-171). Springer, Singapore.
19. Ramanathan, S., Mirkovic, J., Yu, M. and Zhang, Y., 2018, December. SENSS Against Volumetric DDoS Attacks. In *Proceedings of the 34th Annual Computer Security Applications Conference* (pp. 266-277). ACM.
20. Rebecchi, F., Boite, J., Nardin, P.A., Bouet, M. and Conan, V., 2017, July. Traffic monitoring and DDoS detection using stateful SDN. In *Network Softwarization (NetSoft), 2017 IEEE Conference on* (pp. 1-2). IEEE.
21. Sahoo, K.S., Tiwary, M., Sahoo, S., Nambiar, R., Sahoo, B. and Dash, R., 2018, October. Poster: A Learning Automata-based DDoS Attack Defense Mechanism in Software Defined Networks. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking* (pp. 795-797). ACM.
22. Saif, D., Cormier, A., Banik, S. and Matrawy, A., 2018, May. A Review of Recently Emerging Denial of Service Threats and Defences in the Transport Layer. In *2018 IEEE Canadian Conference on Electrical & Computer Engineering (CCECE)*(pp. 1-5). IEEE.
23. Sampigethaya, K., Kopardekar, P. and Davis, J., 2018, April. Cyber security of unmanned aircraft system traffic management (UTM). In *2018 Integrated Communications, Navigation, Surveillance Conference (ICNS)* (pp. 1C1-1). IEEE.
24. Shackelford, S.J. and Brady, A.E., 2017. Is It Time for a National Cybersecurity Safety Board: Examining the Policy Implications and Political Pushback. *Alb. LJ Sci. & Tech.*, *28*, p.56.
25. Shameli-Sendi, A., Pourzandi, M., Fekih-Ahmed, M. and Cheriet, M., 2015. Taxonomy of distributed denial of service mitigation approaches for cloud computing. *Journal of Network and Computer Applications*, *58*, pp.165-179.
26. Singh, N., Hans, A., Kumar, K. and Birdi, M.P.S., 2015. Comprehensive study of various techniques for detecting DDoS attacks in cloud environment. *Int Journal of Grid and Distributed Computing*, *8*(3), pp.119-126.
27. Somani, G., Gaur, M.S., Sanghi, D., Conti, M. and Buyya, R., 2017. DDoS attacks in cloud computing: Issues, taxonomy, and future directions. *Computer Communications*, *107*, pp.30-48.
28. Tama, B.A. and Rhee, K.H., 2015. Data mining techniques in DoS/DDoS attack detection: A literature review. *Information (Japan)*, *18*(8), p.3739.
29. Wang, A., Chang, W., Chen, S. and Mohaisen, A., 2018. Delving into internet DDoS attacks by botnets: characterization and analysis. *IEEE/ACM Transactions on Networking*, *26*(6), pp.2843-2855.
30. Wang, Y., Ma, J., Zhang, L., Ji, W., Lu, D. and Hei, X., 2016. Dynamic game model of botnet DDoS attack and defense. *Security and Communication Networks*, *9*(16), pp.3127-3140.
31. Weagle, S., 2017. Financial Impact of Mirai DDoS Attack on Dyn Revealed in New Data. *Corero Network Security*, *21*.
32. Wirth, A., 2017. Time Flies... and Other Lessons Learned. *Biomed instrumentation & tech*, *51*(2), pp.163-167.
33. Yan, Q., Huang, W., Luo, X., Gong, Q. and Yu, F.R., 2018. A multi-level DDoS mitigation framework for the industrial Internet of things. *IEEE Communications Magazine*, *56*(2), pp.30-36.