International Journal of Research in Engineering, Science and Management
Volume 5, Issue 12, December 2022
https://www.ijresm.com | ISSN (Online): 2581-5792

Rethinking the Acronym of Cybersecurity Operation Center

Demeke Gebresenbet Bayyou*
Assistant Professor, College of Information and Computing Sciences, University of Santo Tomas, Manila, Philippines

***Abstract*: It has been more than half a century since the concept of Cybersecurity Operation Center (SOC) made its way into publication in 1980. Throughout these years there have been many developments in the computing sciences and other fields that use the same acronym SOC. In this paper the infant days of the internet and other areas that are using the acronym SOC are discussed. The integration of Cybersecurity Operation Center to every sector is inevitable, and the usage of search engines is growing. In order to promote better communication and clarity, it is recommendable to use CyOC as acronym (instead of SOC) for Cybersecurity Operation Center.**

***Keywords*: Cybersecurity Operation Center, CyOC, Security Operations Center, SOC.**

1. Introduction

Professor Leonard Kleinrock, the internet architect, together with his team sent the first internet message from the University of California, Los Angeles (UCLA) to the Stanford Research Institute on Oct. 29, 1969 [1]. On one of his interviews published on [2] he discussed about the press release in 1969 at UCLA regarding their achievement. He envisioned that it would be one day possible to access computer services from our homes, just like the way we access electricity and telephone connectivity. However, he did not expect that the access will be as he had observed and thus, he exclaimed, "I never anticipated that my 99-year-old mother would use the Internet at the same time that my 5-year-old granddaughter was—and indeed she did!" He did not mention anything about security at that time, perhaps because he did not imagine the security impact of his invention. After the achievement of this milestone, the internet became a core research area, especially in the United States Department of Defense (DoD).

As the internet developed, it also brought different challenges, and computer security is one of them. Computer security became a concern as early as 1972, which can be traced to the publication of James P. Anderson [3]. In 1980, Anderson in his paper [4] explained in detail the lack of security in the hardware, software systems and applications of that time. He proposed the importance of computer threat monitoring and surveillance system: this can be considered as the birth of Cybersecurity Operation Center (SOC).

There is no clear documentation that shows when the acronym SOC first appeared in publication, but one of the notable things that is repeatedly mentioned in Anderson's paper [4] is the term "Security Officer." The "Security Officer" is described as a person responsible for securing the computer and network system. Since Anderson's team are the early explorers of the area, most probably the acronym also emerged from their research group.

2. Proposal

It has been more than half a century since the concept of Cybersecurity Operation Center (SOC) made its way into publication in 1980. Throughout these years there have been many developments in the computing sciences and other fields that use the same acronym SOC. Some which appeared in scientific literature and other forms of publications are:

- System on Chip (SOC) [5]
- Service-oriented Computing (SOC) [6]
- Selectable Output Control (SOC) [7]

We are witnessing the rapid integration of Information Technology in our daily lives and in all sectors, and it is logical to say that the principle of Cybersecurity Operation Center will also be integrated in every sector. As mentioned, the acronym SOC describes many other concepts apart from Cybersecurity Operation Center. Moreover, the internet community use search engines to learn about any topic under the sun, and the acronym SOC is not differentiated by search engines. If one searches for SOC, search engines can give results that are related to "System on Chip," "Service-oriented Computing," "Selectable Output Control," or "Cybersecurity Operation Center." Therefore, for better communication and clarity, it is recommendable to use CyOC for Cybersecurity Operation Center, instead of SOC.

The acronym CyOC was used for the first time in 2018, when NATO member states agreed on how to integrate sovereign cyber effects, provided voluntarily by Allies, into Alliance operations and missions, as well as to setup the initial Cyberspace Operations Centre [8].

Google trends was used to observe the comparison of the search trends of the two terms, "Cybersecurity Operation Center" and "System on Chip," from January 30, 2020 until the preparation of this research. As shown in Figure 1, the latter one is the most searched term during the selected period. The search trend of "SOC" using Google trends was also observed. As shown in Figure 2, the result speaks louder that the search trend

*Corresponding author: demeke.g.bayyou@ieee.org

of the "SOC" is more than the combined search trends of "Cybersecurity Operation Center" and "System on Chip".

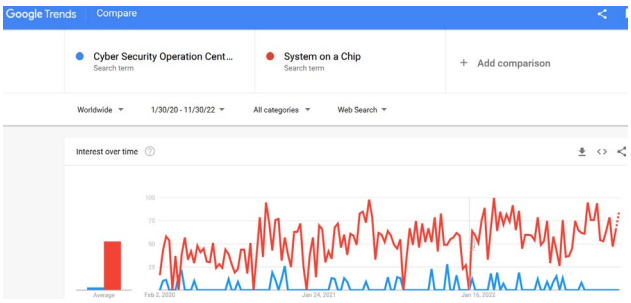

Fig. 1. Search trends for Cyber Security Operation Center and System on Chip

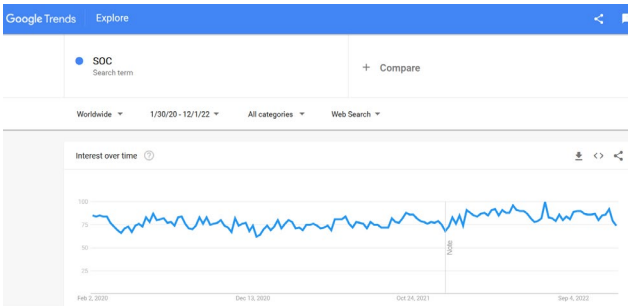

Fig. 2. Search trends for SOC

3. Conclusion

The acronym SOC will continually be used in different fields other than the Computing Sciences, and it may even be used in fields which will be invented in the future. The integration of Cybersecurity Operation Center to every sector is inevitable, and the usage of search engines will continue to grow. Therefore, for better communication and clarity for the internet community and for the search engines, it is recommendable to use CyOC instead of SOC as an acronym for Cybersecurity Operation Center.

References

[1] "Internet Architect Dr. Leonard Kleinrock Receives UCLA Medal", UCLA Samueli Newsroom, Feb 24, 2020. https://samueli.ucla.edu/internet-architect-dr-leonard-kleinrock-receives-ucla-medal/

[2] James F. Kurose and Keith W. Ross, "Computer Network A Top-Down Approach", Pearson, 8th edition, 2021.

[3] Anderson, J. P., Computer Security Technology Planning Study, ESD-TR-73-51, ESD/AFSC, Hanscom AFB, Bedford, MA, Oct. 1972. https://seclab.cs.ucdavis.edu/projects/history/papers/ande72a.pdf

[4] Anderson, J. P., Computer Security Threat Monitoring and Surveillance, James P. Anderson Co., Fort Washington, PA ,1980 https://seclab.cs.ucdavis.edu/projects/history/papers/ande80.pdf

[5] Partha Pratim Pande, Cristian Grecu, Andri Ivanov, Res Saleh, Design of a Switch for Network on Chip Applications, Proceedings of the 2003 International Symposium on Circuits and Systems. ISCAS '03.

[6] Mike P. Papazoglou, Service-Oriented Computing: Concepts, Characteristics and Directions, Proceedings of the Fourth International Conference on Web Information Systems Engineering, 2003.

[7] EFF Opposes MPAA's Selectable Output Control FCC Petition, Electronic Frontier Foundation, 2008. https://www.eff.org/deeplinks/2008/07/eff-opposes-mpaas-selectable-output-control-fcc-pe

[8] Laura Brent, NATO's role in cyberspace, 2019. https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html