AN APPROACH TO CYBER RESILIENCE OF CRITICAL INFORMATION INFRASTRUCTURES

Kashaija Joel, Massis Khader, Onuoha David Nwaezeudo

Kharkiv National University of Radio Electronics,
Ukraine

E-mail: kashaija.joel@nure.ua,
khader.massis@nure.ua,
devid.nvaezeudo.onuokha@nure.ua

Abstract

The paper is devoted to an approach to cyber resilience of Critical Information Infrastructures. The cyber resilience of networked services becomes especially important because in many cases such services will increasingly be offered by mission-critical applications. They will need guarantees above and beyond the 'best effort' that has initially been considered acceptable for applications provided by conventional networks. Moreover, mission-critical networks must continue to operate during any disaster and protect sensitive information and guard against attacks.

The fast-changing world of information and communication technologies (ICT) introduces new cybersecurity-related risks to critical infrastructures (CI), critical information infrastructures (CII), essential services (Table 1), and societies in general [1-3]. Nations are creating CI protection and cyber resilience related laws, regulations, frameworks, and strategies to mitigate and manage cyber risks [2, 3].

It should be mentioned that cyber resilience generally refers to the ability of a system to restore its normal behavior, thus overcoming the deterioration of performance after cyberattacks, antagonistic impact, etc. Accordingly, cyber resilience is becoming a viable tool, especially for critical infrastructures.

Typically, critical information infrastructure objects are identified in the following order [4]:

- the operator of essential services defines all objects of information infrastructure (automated, information, telecommunication, information-telecommunication systems, automated control systems of technological processes), which are operated on the object of critical infrastructure;
- the operator of the essential services determines which of the above information infrastructure facilities are necessary to ensure the continuous and sustainable operation of the critical infrastructure facility in terms of providing it with essential services and evaluates their criticality.

Table 1. Critical sectors and related critical services [3]

Sector	Subsector	Service
Information and Communication Technologies (ICT)	Information Technologies	Web services
		Datacenter/Cloud services
		Software as a Service (SaaS)
	Communications	Voice/Data communication
		Internet

In turn, any network must have the ability to provide and maintain a level of services to face challenges, failures, and attacks with resilience, fault tolerance, and survivability [5-10].

Mission Critical Network Architecture reliability is concerned with the following. Mission-critical networks must continue to operate during any disaster, including hurricanes, earthquakes, fires, or high-powered blasts caused by a bomb [1, 4]. While in terms of cyber security, public safety agencies need to protect sensitive information and guard against attacks that could take down the network.

The Mission Critical Network developing and deploying has a complete set of requirements, which provides the platform for all the other architecture building blocks and a collection of integrated network services. The services cover resiliency, network virtualization, compute, storage, traffic optimization,

mobility and location, management and monitoring, identity, unified communications, application networking, and security [7-10].

Here reliability refers to the quality of voice, video, and data. Resiliency services include Quality of Service (QoS) to assign priority to delay-sensitive traffic [7]. They also require adequate network performance (bandwidth). In terms of redundancy, if one network is destroyed or unavailable, personnel at the incident scene need another means of access at the incident scene. Many organizations use wireless or satellite networks as a fallback. While survivability refers to maintaining command-and-control operations at the incident even if all redundant networks become unavailable, it can be achieved by establishing an ad hoc meshed network between all remaining nodes.

Lastly, the Mission Critical Network specifies the design for places requiring network connectivity, such as data centers, nationwide networks, headquarters, remote posts, the mobile workforce, the homes to critical servers, storage, and applications, and many more.

Therefore, the cyber resilience of networked services becomes especially important because in many cases, such services will increasingly be offered by mission-critical applications. They will need guarantees above and beyond the 'best effort' that has initially been considered acceptable for applications provided by conventional networks.

References

1. *Rak J., Hutchison D. (eds)* Guide to Disaster-Resilient Communication Networks. Computer Communications and Networks. Springer, Cham. 2020. 813 p. DOI: https://doi.org/10.1007/978-3-030-44685-7.

2. *Luiijf E., Klaver M.* Resilience Approach to Critical Information Infrastructures. In: Gritzalis D., Theocharidou M., Stergiopoulos G. (eds) Critical Infrastructure Security and Resilience. Advanced Sciences and Technologies for Security Applications. Springer, Cham. 2019. P. 3-16. DOI: https://doi.org/10.1007/978-3-030-00024-0_1.

3. *Petrakos N., Kotzanikolaou P.* Methodologies and Strategies for Critical Infrastructure Protection. In: Gritzalis D., Theocharidou M., Stergiopoulos G. (eds) Critical Infrastructure Security and Resilience. Advanced Sciences and Technologies for Security Applications. Springer, Cham. 2019. P. 17-33. DOI: https://doi.org/10.1007/978-3-030-00024-0_2.

4. Executive White Paper. Cisco Open Platform for Safety and Security: Understand the Mission-Critical Network Architecture Building Block. URL: https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/COPSSMission-CriticalNetwork_wp.pdf

5. *Shirazi S.N., Gouglidis A., Farshad A., Hutchison D.* The extended cloud: Review and analysis of mobile edge computing and fog from a security and resilience perspective. IEEE Journal on Selected Areas in Communications. 2017. Vol. 35, No.11. P. 2586-2595. DOI: https://doi.org/10.1109/JSAC.2017.2760478.

6. *Sterbenz J. P. G.* Smart city and IoT resilience, survivability, and disruption tolerance: Challenges, modelling, and a survey of research opportunities. *2017 9th International Workshop on Resilient Networks Design and Modeling (RNDM)*, Alghero. 2017. P. 1-6. DOI: https://doi.org/10.1109/RNDM.2017.8093025.

7. *Lemeshko O., Yeremenko O., Shapovalova A., Hailan A. M., Yevdokymenko M., Persikov M.* Design and Research of the Model for Secure Traffic Engineering Fast ReRoute under Traffic Policing Approach. *2021 IEEE 16th International Conference on the Experience of Designing and Application of CAD Systems (CADSM).* 2021. P. 23-26. DOI: https://doi.org/10.1109/CADSM52681.2021.9385253.

8. *Lemeshko O., Yeremenko O., Yevdokymenko M., Shapovalova A., Lemeshko V.* Network Security Approach Based on Traffic Engineering Fast ReRoute with support of Traffic Policing. Proceedings of the Selected Papers on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2021). Kyiv, Ukraine. CEUR, 2021. Vol. 2923. P. 81-90.

9. *Yeremenko O. S., Ali S. A.* Secure Multipath Routing Algorithm with Optimal Balancing Message Fragments in MANET. Radioelectronics and Informatics. 2015. No 1 (68). P. 26–29.

10. *Yeremenko O., Lemeshko O., Persikov A.* Secure Routing in Reliable Networks: Proactive and Reactive Approach. Advances in Intelligent Systems and Computing II, CSIT 2017, Advances in Intelligent Systems and Computing, Springer, Cham. 2018. Vol. 689. P. 631–655. DOI: https://doi.org/10.1007/978-3-319-70581-1_44.