# 网络安全时代的机遇与风险

# 一．期刊十篇

1.[1]赵蓉英,常茹茹,李丹阳,戴祎璠.基于ATM模型的专利权人话语权评价研究——以网络安全领域为例[J/OL].情报理论与实践:1-13[2021-10-13].http://kns.cnki.net/kcms/detail/11.1762.g3.20211012.1524.004.html.

2.[1]吴小伟.“等保2.0”背景下政府部门网络信息安全防护技术探析[J].江苏科技信息,2021,38(32):39-41.

3.[1]张兆阳,常茹茹,李丹阳,戴祎璠,赵蓉英.网络安全领域专利权人话语权评价：框架与模型[J/OL].情报理论与实践:1-16[2021-10-13].http://kns.cnki.net/kcms/detail/11.1762.g3.20211008.1859.002.html.

4.[1]冼进,冼允廷.高校网络信息安全实验室建设探索[J].福建电脑,2021,37(10):40-44.

5.[1]冼进,冼允廷.高校网络信息安全实验室建设探索[J].福建电脑,2021,37(10):40-44.

6.[1]朱伊华.智能楼宇系统中网络安全技术分析[J].中国设备工程,2021(19):31-32.

7.[1]胡蕊.青少年社交网络安全的法规分析：防护、保障与监管[J].北京青年研究,2021,30(04):44-49.

8.[1]刘艳.计算机网络信息安全及其防火墙技术应用[J].互联网周刊,2021(19):43-45.

9.[1]郝俊祥.企业信息化建设网络安全威胁分析[J].中国管理信息化,2021,24(19):93-95.

10.[1]郑楠.信息化时代计算机网络安全探索[J].中国科技信息,2021(19):52-53.

**二：论文两篇**

[1]史冯琪. 网络服务提供者安全保障义务与侵权责任[D].沈阳师范大学,2021.

[1]李天南. 5G网络个人信息安全伦理探析[D].沈阳师范大学,2021.

**三：外文文献**

# AI-assisted Computer Network Operations testbed for Nature-Inspired Cyber Security based adaptive defense simulation and analysis

## Highlights

•

Demonstrated a network test-bed for Cybersecurity attacks and defense.

•

Special features for testing Nature-inspired and Artificial intelligence based algorithms.

•

Provide easy configuration and setup option for carry out advanced attacks and defense.

•

Comprehensive reporting and visualization.

•

Experiments and result are shown for two real time use-cases example Distributed Denial of Service Attack(DDoS).

## Abstract

In the current ever-changing cybersecurity scenario, active cyber defense strategies are imperative. In this work, we present a standard [testbed](https://www.sciencedirect.com/topics/computer-science/testbed" \o "Learn more about testbed from ScienceDirect's AI-generated Topic Pages) to measure the efficacy and efficiency of customized networks while analyzing various parameters during the active attack. The presented testbed can be used for analyzing the network behavior in presence of various types of attacks and can help in fine-tuning the proposed algorithm under observation. The proposed testbed will allow users to design, implement, and evaluate the active cyber defense mechanisms with good library support of nature-inspired and AI-based techniques. Network loads, number of clusters, types of home networks, and number of nodes in each cluster and network can be customized. While using the presented testbed and incorporating active-defense strategies on existing [network architectures](https://www.sciencedirect.com/topics/computer-science/network-architecture" \o "Learn more about network architectures from ScienceDirect's AI-generated Topic Pages), users can also design and propose new network architectures for effective and safe operation. In this paper, we propose a unified and standard testbed for cyber defense strategy simulation and bench-marking, which would allow the users to investigate current approaches and compare them with others, while ultimately aiding in the selection of the best approach for a given [network security](https://www.sciencedirect.com/topics/computer-science/network-security" \o "Learn more about network security from ScienceDirect's AI-generated Topic Pages) situation. We have compared the network performance in difference scenarios namely, normal, under attack and under attack in presence of NICS-based adaptive defense mechanism and achieved stable experimental results. The experimental results clearly show that the proposed testbed is able to simulate the network conditions effectively with minimum efforts in [network configuration](https://www.sciencedirect.com/topics/computer-science/network-configuration" \o "Learn more about network configuration from ScienceDirect's AI-generated Topic Pages). The simulation results of defense mechanisms verified on the proposed testbed got the improvement on almost 80 percent while increasing the turnaround time to 1–2 percent. The applicability of proposed testbed in modern technologies like [Fog Computing](https://www.sciencedirect.com/topics/computer-science/fog-computing" \o "Learn more about Fog Computing from ScienceDirect's AI-generated Topic Pages) and Edge Computing is also discussed in this paper.

# Security factors on the intention to use mobile banking applications in the UK older generation (55+). A mixed-method study using modified UTAUT and MTAM - with perceived cyber security, risk, and trust

## Highlights

•

Less than half of 55+ intend to use a mobile banking application in next 3 months.

•

Performance expectancy and perceived cyber security risk influence intention to use.

•

Effort expectancy, cyber security trust and overall security were insignificant.

•

The model explains 87% of the variance for the sample.

## Abstract

The convenience and accessibility of mobile banking applications has resulted in this becoming the preferred method of banking in the UK. Although popular amongst a younger generation, uptake is significantly lower among the older generation of those aged 55+, with some attributing this to cyber security and privacy concerns.

This study proposes a model that can be used to measure the influence of cyber security factors on intention to use mobile banking applications, in the UK 55+. The unified theory of acceptance and use of technology (UTAUT) model was modified to include perceived cyber security risk, perceived cyber security trust, and perceived overall cyber security. Unlike similar studies which have been solely quantitative, this research brings further insight using a mixed-methods approach which harnesses both qualitative and quantitative data.

The research model was tested using partial-least-squares structural equation modelling on coded questionnaire data, collected from 191 participants. Qualitative data was analysed through a thematic analysis. Both sets of data were analysed using a final convergent mixed-method. The results show that performance expectancy followed by perceived cyber security risk are the main determinants of intention to use mobile banking applications in the UK 55+.