Scientific and Practical Cyber Security Journal (SPCSJ) 6(1): 59-63 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

THE GLOBAL CYBERSECURITY INDEX (GCI) ACCORDING TO A RECENT STUDY

Tinatin Mshvidobadze Professor Gori State University (Georgia)

ABSTRACT: The paper illustrates and analyzes the data of the International Telecommunication Union (ITU) survey on the Global Cyber Security Index. The model of the new concept of information security is offered. It is described and analyzed in the paper how countries can consider the use of the ITU Guide to Developing a National Cybersecurity Strategy as a toolkit to support the creation or enhancement of their national strategy. The comparison of global IDI and GCI ranking by different countries is also offered in the paper.

KEYWORDS: *Information society, Development Index, Cybersecurity, GCI.*

The ICT Development Index

Society is challenged by the information cyber threats such as denial of e-services, data integrity breaches, and data confidentiality breaches, and the effectiveness of the Internet is linked to cybersecurity as more countries are advancing in the use of ICTs.

In such ~~a~~ situation, an advanced protection solution is needed. Not long ago, vendors introduced a new platform that will facilitate the identification, analysis of incidents and helped block to attack. The concept will allow information security specialists to see the entire spectrum of threats, even events that were not included in the field of view of security experts.

XDR (Extended Detection and Response) - advanced detection, responses the threats of complex levels and targeted attacks. The system is aimed at working not only with endpoints, but also focuses on the analysis of network traffic, e-mail, cloud complex of structures.

The innovative new XDR concept continues to evolve gradually to provide comprehensive information security. The platform quickly processes a huge array of logs, responds quickly and in a timely manner to incidents. XDR can also be combined with SIEM / SOAR work models to speed up incident handling.

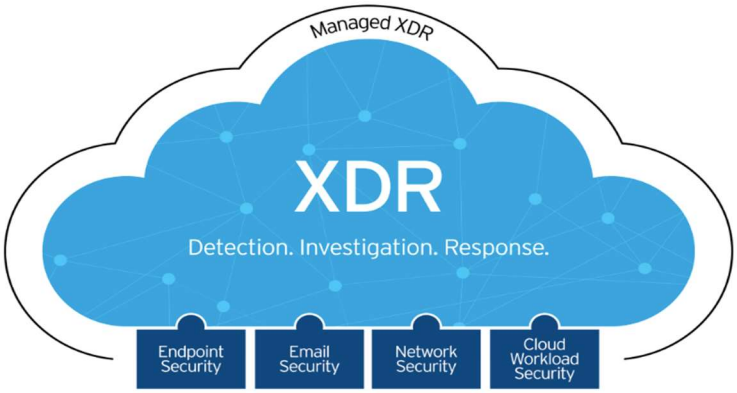

Fig.1. system XDR

The ICT Development Index (IDI) has been produced and published annually by International Telecommunication Union (ITU) since 2009. It is a composite index that combines 11 indicators into one benchmark measure. It is used to monitor and compare developments in the information and communication technology (ICT) between countries and over time. The report features key ICT data and a benchmarking tool to measure the information society, the ICT Development Index (IDI).[1]

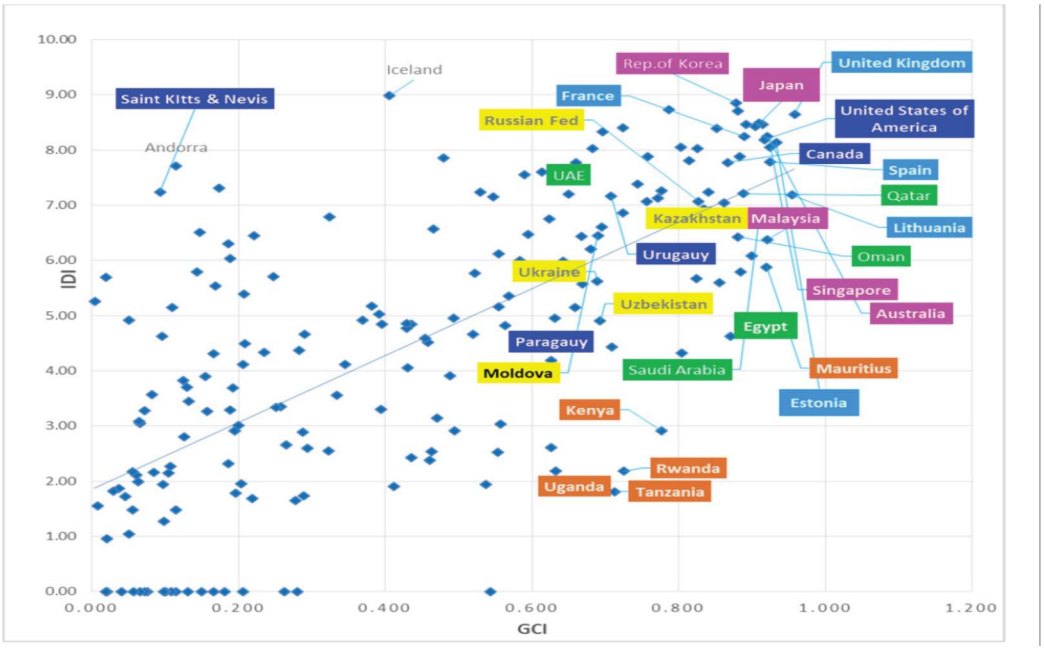

Fig.2. Comparison of global IDI and GCI ranking

[1] https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2017.aspx

Figure 2 shows that not all countries with high IDI scores have a similarly high score in GCI, for instance Iceland took the top place in IDI scoring 8.98 while only 0.406 in the GCI. Andorra, and Saint Kitts and Nevis, also score high in IDI and yet very low in GCI, although some countries are maintaining their leading positions in both indices.

Global Cyber Security Index (GCI) According to a 2020 study

Japan – The Japan National center of Incident readiness and Strategy for Cybersecurity (NICS) is building an information sharing system among public-private sectors[2]. The Japan National Institute of Information and Communication-Technology has established a National Cyber Training Center that has developed many projects, such as CYDER, CYBER COLOSSEO and Sec Hack 365 (a security innovator training program for young talents).

Lithuania - To consolidate functions and resources, which were previously scattered among various institutions into single entity, the National Cyber Security Centre (NCSC)[3] has been created. Consolidation has helped to concentrate best expertise and avoid not always efficient inter-institutional interaction issues, thus enabling faster decision-making and response time. The National Cyber.

Malaysia - Best practice guidelines have been developed for security services and cloud security practice in collaboration with the industry [1]. A cloud security practice document is being prepared to establish a cloud security certification scheme. An Internet Banking Task Force, consisting of local financial institutions, the Malaysian Communications and Multimedia Commission (MCMC), Cybersecurity Malaysia, and the Royal Malaysian Police, is being established to combat online banking fraud [4].

According a framework of Information Security Management System (ISMS) The Digital Forensics Working Group, comprising all law enforcement agencies that operate digital forensic laboratories, is being created. [2]

Singapore – The public and private sectors in Singapore have worked together to develop or adopt new cybersecurity standards to address gaps in cybersecurity standards. According to Irene Tham this new standard caters for different levels of security, depending on the level that service providers can offer to their users. The Singapore Standards Council has also embarked on the development of new standards that are currently not available at the international level. These include cybersecurity standards for autonomous vehicles and general requirements for IoT security for smart nation projects in Singapore [3].

[2] https:// www .nisc .go .jp/ eng/

[3] https://www.nksc.lt/en/

[4] https://www.cybersecurity.my/data/content_files/11/1170.pdf?.diff=1375349394

United Kingdom – The NCSC Active Cyber Defense Program aspires to protect the majority of people in the United Kingdom. Four initial measures have already had a significant impact: blocking fake emails; stopping systems veering into malicious websites; helping organizations easily fix website problems; phishing and malware mitigation. The program is expected to continue to drive change over the next two to five years. The NCSC launched Active Cyber Defense, which has prevented thousands of attacks and reduced the average time a phishing site is online from 27 hours to 1 hour. There has been a 43 percent increase in visits to the Cyber Security Information Sharing Partnership (CiSP), which allows the community to share information about cyber threats.[5]

Ukraine – The CERT-UA[6] team is constantly taking steps to engage with other Member State CERT teams, as well as with the Cisco Talos Intelligence Group on issues related to overcoming the effects of cyber-attacks on critical information infrastructure and identifying the causes and circumstances of cyber incidents.

Moldova – In the context of the development of information society aspirations, the Government of the Republic of Moldova approved a strategic and legislative framework for the development of the ICT domain in Moldova, the most important being the National Strategy for Information Society Development "Digital Moldova 2020" [4].

Georgia started a cyber research project in 2018, a Portal of Online Cyber exercises[7]. Cyber Lab – a new online resource created by Computer Emergency Response Team (CERT.GOV.GE) and Georgian Research and Educational Networking Association (GRENA) with the support of EU funded EaP- Connect project. The portal helps IT students from educational institutions interested in cybersecurity to deepen their practical skills, so they can better discover and then respond to cyber incidents. The portal will also help IT personnel from both the public and private sectors, where readiness is critically important to defend against attack, ensure cyber sustainability, and improve skills[5].

CONCLUSION

Measuring progress towards the cybersecurity commitment of countries globally is a complex task which entails striking a balance between different dimensions of cybersecurity experiences in different countries.

[5] https://www.ncsc.gov.uk/section/active-cyber-defence/introduction

[6] https:// cert .gov .ua/

[7] www .cyberlab .tech

The GCI originally succeeded in measuring commitment to cybersecurity and generated interest on cybersecurity assessment among countries.

The GCI continues to contribute to the cybersecurity awareness in the least developed countries providing capacity building activities through the production of guidelines on cybersecurity legislation, regulation and technology, asserting the need and importance for countries to establish national computer incident response teams (CIRTs) and providing fundamental tools to develop a national cybersecurity strategies.

REFERENCES:

1. ISO/IEC DIS 27001:2018, Information technology - Security techniques - Information security management systems – Requirements;

2. ISO/IEC DIS 27002:2018, Information technology - Security techniques - Code of practice for information security controls;

3. Irene Tham, Campaign to ready public servants for Internet separation, https://www.straitstimes.com/singapore/campaign-to-ready-public-servants-for-internet-separation%20;

4.О Национальной стратегии развития информационного общества «Цифровая Молдова 2020», ПОСТАНОВЛЕНИЕ Nr. 857, http://lex.justice.md/viewdoc.php?action=view&view=doc&id=350246&lang=2

5. Maksim Iavich, Sergiy Gnatyuk, Giorgi Iashvili, Andriy Fesenko, Cyber security European standards in business, Scientific and practical cyber security journal, 2019