



**VILNIUS UNIVERSITY
ŠIAULIAI ACADEMY
BACHELOR PROGRAMME SOFTWARE ENGINEERING**

**Modelling in Software System Development
Project Draft**

“Prevention of internet scamming and fraud in Ukraine”

Group members: Daniil Arbatov, Hanna
Asiadouskaya, Ivan Kapusta, Yasin Zakhedul Islam,
Artem Shymko

Lecturer: dr. Mykolas Okulič-Kazarinas

Šiauliai, 2024

Issue

In the Ukraine the scamming and fraud on the internet causes a lot of trouble for the people. A lot of money is stolen every single day, the plenty of cases still remain unsolved, people are still falling for calls from various “bank managers” with the voice changer software. So, today our group will try to analyse the issue and find the solutions using system dynamics.

System

Research in governmental scale of systematic occurrence of scamming cases in Ukraine

Goal

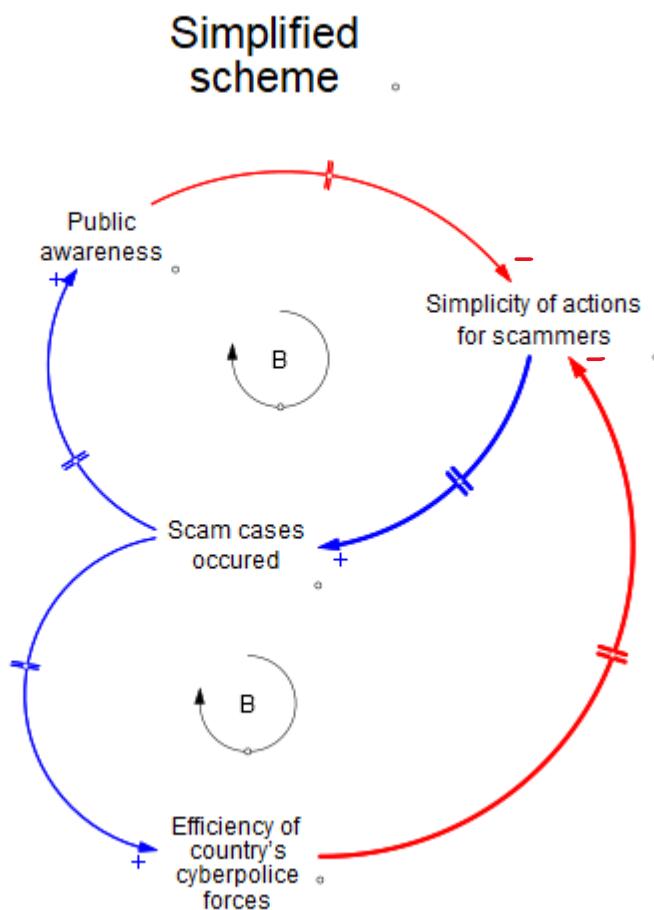
To cut the number of occurred internet scam cases in half by the end of 2030

Factors

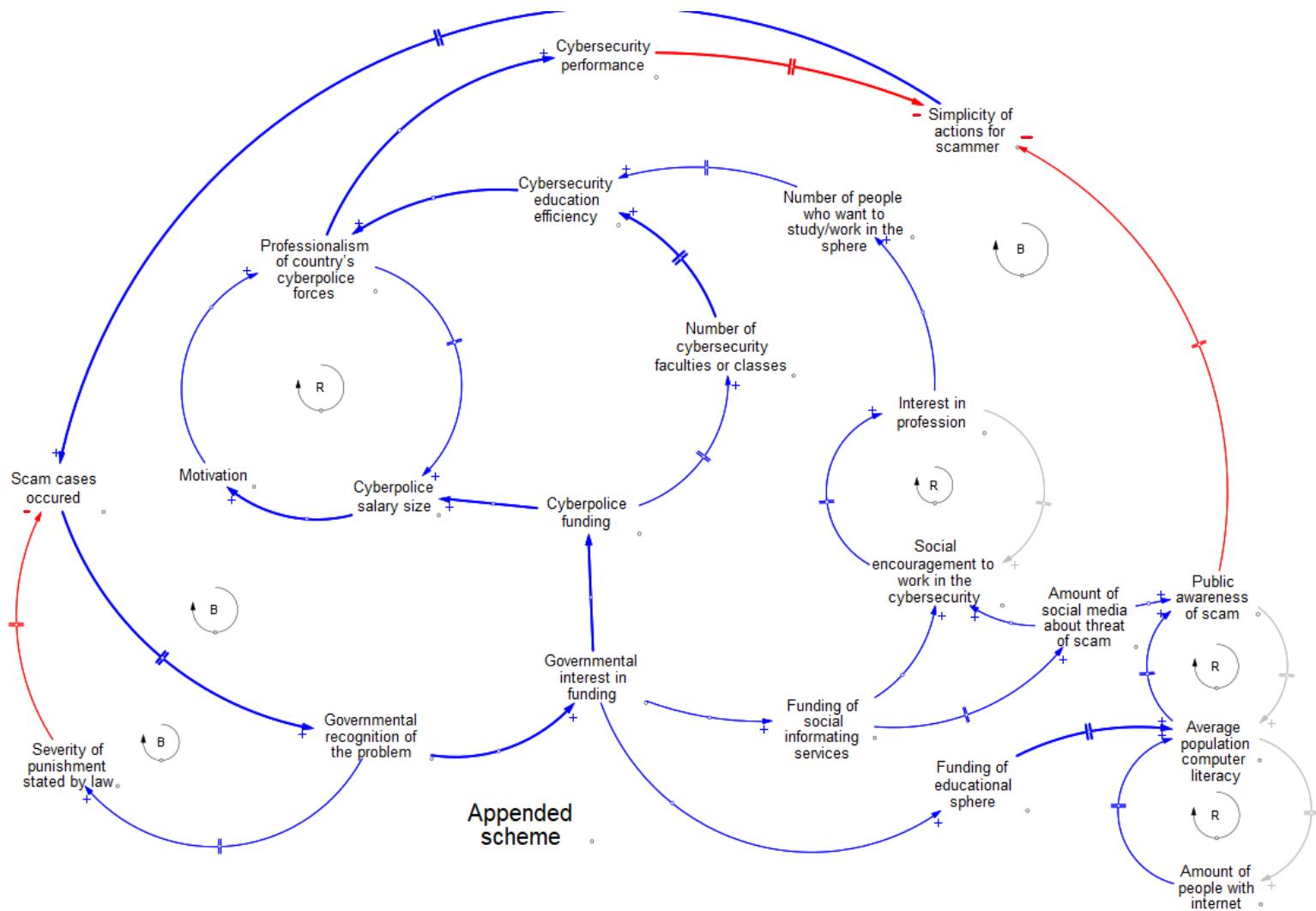
1. Development and efficiency of country's cyberpolice forces.
 - 1.1. Amount of governmental funding of the internet security police department that results in salaries of the cybersecurity workers, which will affect the motivation of people to efficiently do their job. (Can be measured by the correlation between the salary size and motivation, which would be represented using surveys of workers)
 - 1.2. Number of schools, universities, and educational centres, where the cybersecurity is studied. (Can be measured by the number of faculties or classes, which relate to the subject)
 - 1.3. Social encouragement to work and study in the field of cybersecurity, which will affect the number of potential specialists. (Can be measured by the number of people who know about the profession and the number of people who want to study/work in the sphere)
2. Awareness of civilians.
 - 2.1. Level of basic computer literacy of the vulnerable social groups, such as elderly or underage people. (Can be measured by offering various test-like surveys on the streets)
 - 2.2. Number of educational centres or school classes where the basic computer science can be studied.
 - 2.3. Amount of people with internet access.
 - 2.4. Quantity of social media about the threat of scamming.

3. Simplicity of actions for scammer.
 - 3.1. Cybersecurity performance, or speed of reaction and capture. (Can be measured by mean time to locate the scammer and arrest him)
 - 3.2. Quantity of available technologies with unrestricted unauthorized access which could assist the scammer. Such as voice-changers, keygainers, look-changers.
 - 3.3. The severity of punishment if caught. (Can be measured by number of fines or years of imprisonment stated by the law)
 - 3.4. Social organization and public awareness (Represent amount of confidence of people, knowledge of the threat and the trust in government. Can be affected by the country corruption, internal struggles, or ongoing wars)

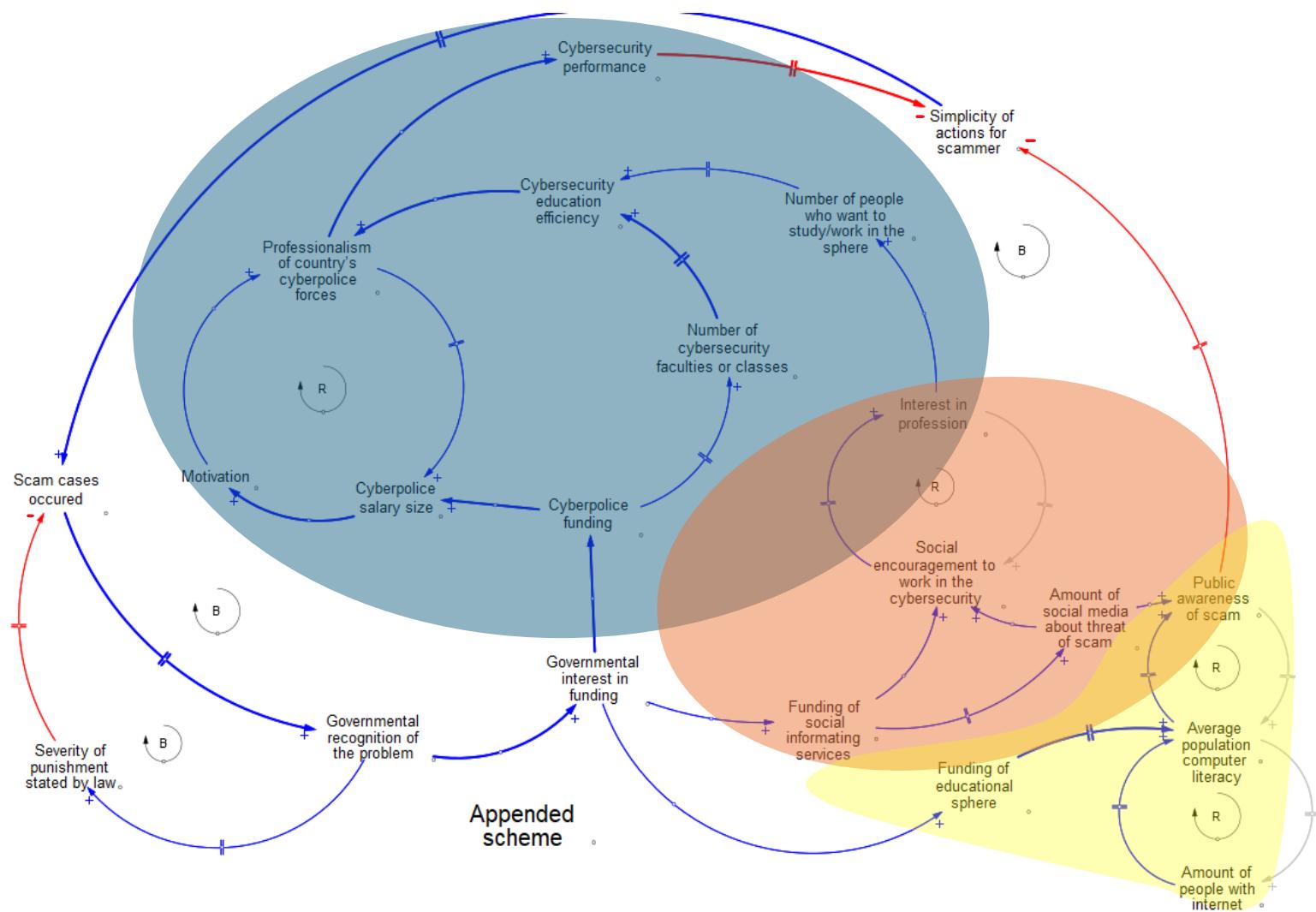
Simplified Scheme:



Appended Scheme:



Main spheres:



- ➊ Cyberpolice influence focused sphere.
- ➋ Social media influence focused sphere.
- ➌ Education influence focused sphere.

Conclusion

Overall, this system might be considered stable. The presence of negative (balancing) loops proves the statement. System tends to balance itself by the course of revolution of relations between various factors, some of those are bend into the reinforcement loops, but the most influential tend to be those from balancing loops:

- A) [Scam cases occurred → Public awareness → Simplicity of actions for scammers → Scam cases occurred.]
- B) [Scam cases occurred → Efficiency of Cyberpolice → Simplicity of actions for scammers → Scam cases occurred.]

In the model the most engaged aspect tends to be the funding of the Cyberpolice forces. It more or less directly influences the most important model aspects, as well as has strong relations without delays with the target. So, the increase of this factor, especially because of the presence of the reinforcement loop [**Cyberpolice salary size** → **Motivation** → **Professionalism**], will lead to the most rapid changes in the model.

The alternative roots of funding the Educational sphere or Social information services also proved to be effective, but, the considerable amount of delays and more weak connections. Increase of funding in these spheres will not have such a rapid impact on the solution of a problem, but will surely be helpful, because of the presence of two semi-weak reinforcing loops [**Average computer literacy** → **Amount of people with internet**] and [**Average computer literacy** → **Public awareness of scam**]

To cut a long story short, the optimal solution of the problem needs to involve at least two of the funding spheres, one of which needs to be Cyberpolice. For example, increasing the Social media influence will affect **Scam Cases Occurred** through **Public awareness** and the minor improvements of the Cyberpolice area; increased **Educational funding** will just increase **Public awareness**, but the changes will be more rapid. Coupled with the **Cyberpolise funding**, one of those solutions will lead to rapid decrease of **Occurred scam cases**. Eventually, the problem would be almost completely solved, and if the same level of funding will remain, will not appear again.

Sources

Anita Prasad (2024) The number of open cases related to fraud.

<https://forbes.ua/ru/news/v-ukraini-zrostae-riven-shakhraystva-torik-kilkist-vidkritikh-sprav-syagnula-istorichnogo-maksimumu-opendatabot-21022024-19351>

Visa Media (2023) Stay Secure CEMEA Study

https://km.visamiddleeast.com/en_KM/pay-with-visa/security-and-assistance/stay-secure.html#3

Lisa Palchynska (2021) How Ukrainians are being deceived on the Internet

<https://ain.ua/ru/2021/08/26/v-2021-godu-ukrainczy-vdvoe-chashhe-stalkivayutsya-smoshennichestvom-v-internete-issledovanie-olx/>