ALTERNATIVE NATIONAL CYBERSECURITY SYSTEM IN UKRAINE

KOSTIANTYN KORSUN,

NGO UISG, HEAD OF COUNCIL; BEREZHA SECURITY, CEO

UADOM, DECEMBER 7, 2018, KYIV, UKRAINE

SAD REALITY: CURRENT NATIONAL CYBERSECURITY SYSTEM IN UKRAINE DOESN'T WORK.

Why?

Six Main Entities of National Cybersecurity System + RNBO: not coordinated

Operate in their own discretion

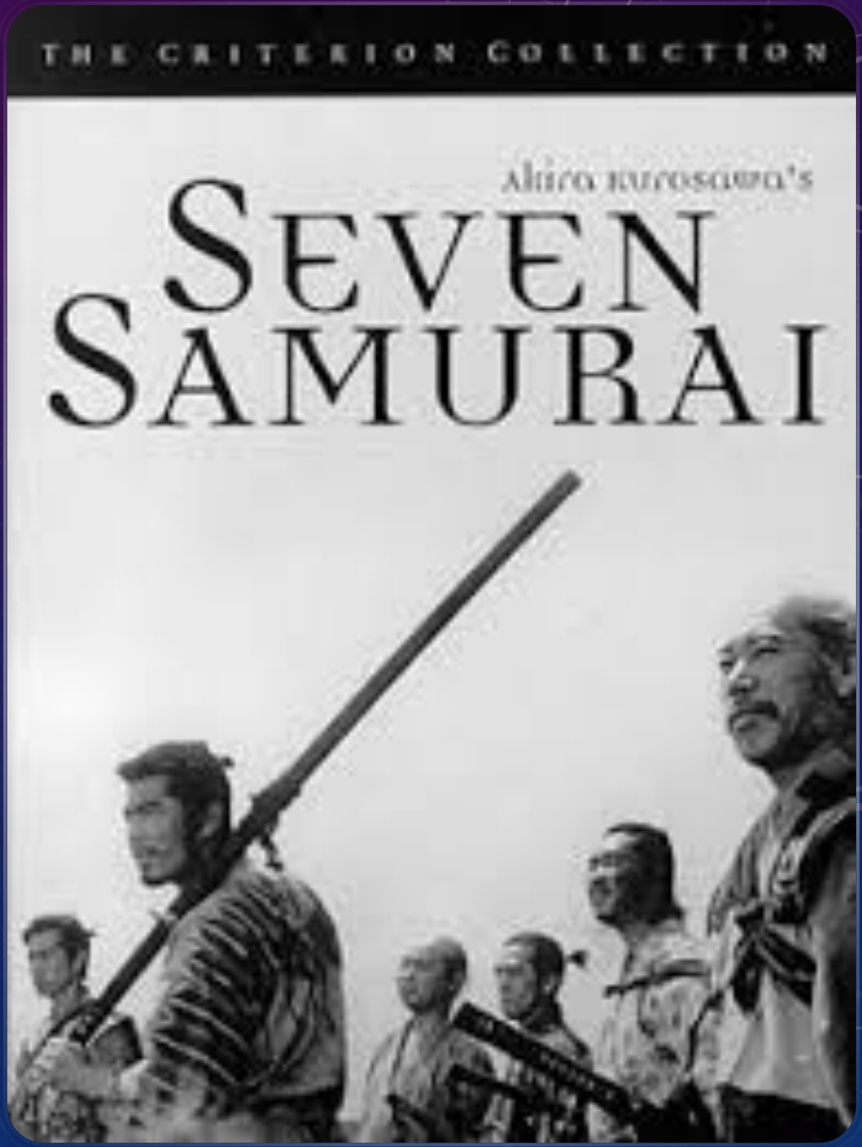
Lack of trust to the Main Entities

Professional level: low

Ambitions: high

Budgets: waste of money/absence

International support: not effective



SAD REALITY: CURRENT NATIONAL CYBERSECURITY SYSTEM IN UKRAINE DOESN’T WORK.

What the problem?

Government wants but can’t (lack of proper people)

Cyber business and cyber community could help but are not motivated; + no authority

Public-Private Partnership doesn’t work

The West wants to help however contacts only Government

Corruption

More detailed: https://www.slideshare.net/KostiantynKorsun/ybersecurity-system-in-ukraine-reality-or-myth?fbclid=IwAR124o2egWHjqRg4wH2OOLdXXTkMkltyGhuyGwJcJH8tk_5T5LyJdi5BcTE

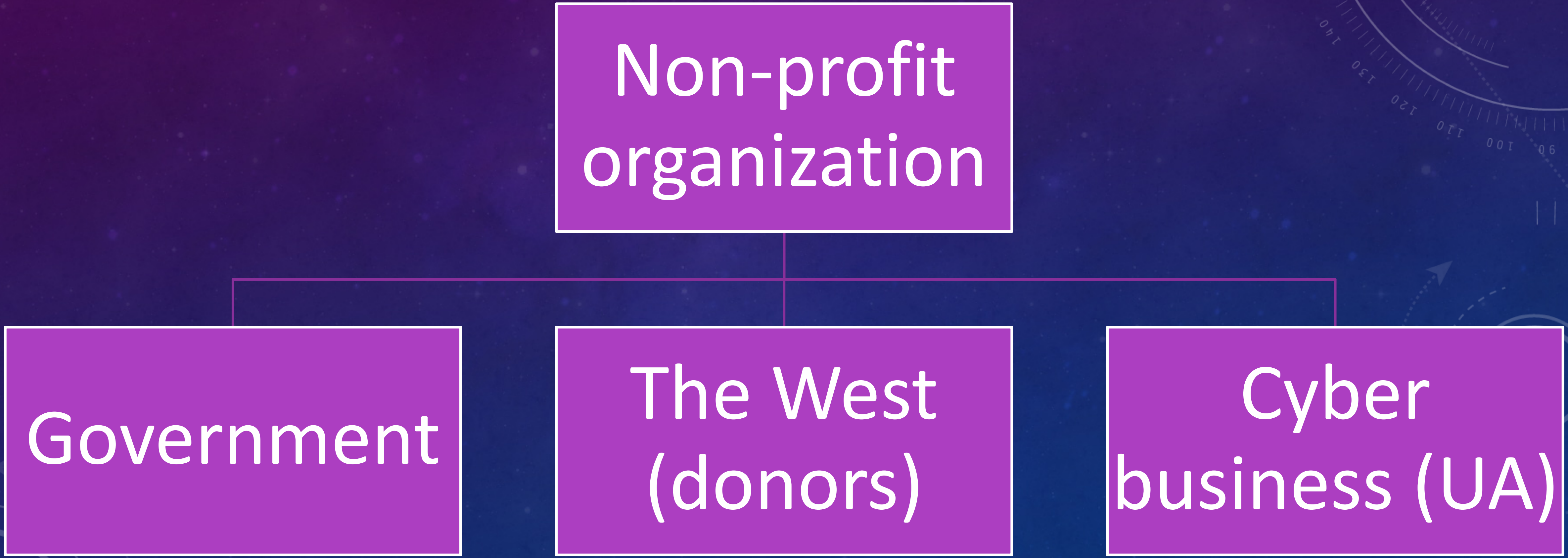
ВИХОДУ
НЕМА
?

HOW TO FIX IT?

5 main principles:

1. Current System can not be fixed
2. Current System should not be destroyed
3. New System should be built in parallel
4. People is our All
5. Trust is the main goal

THE MATTER



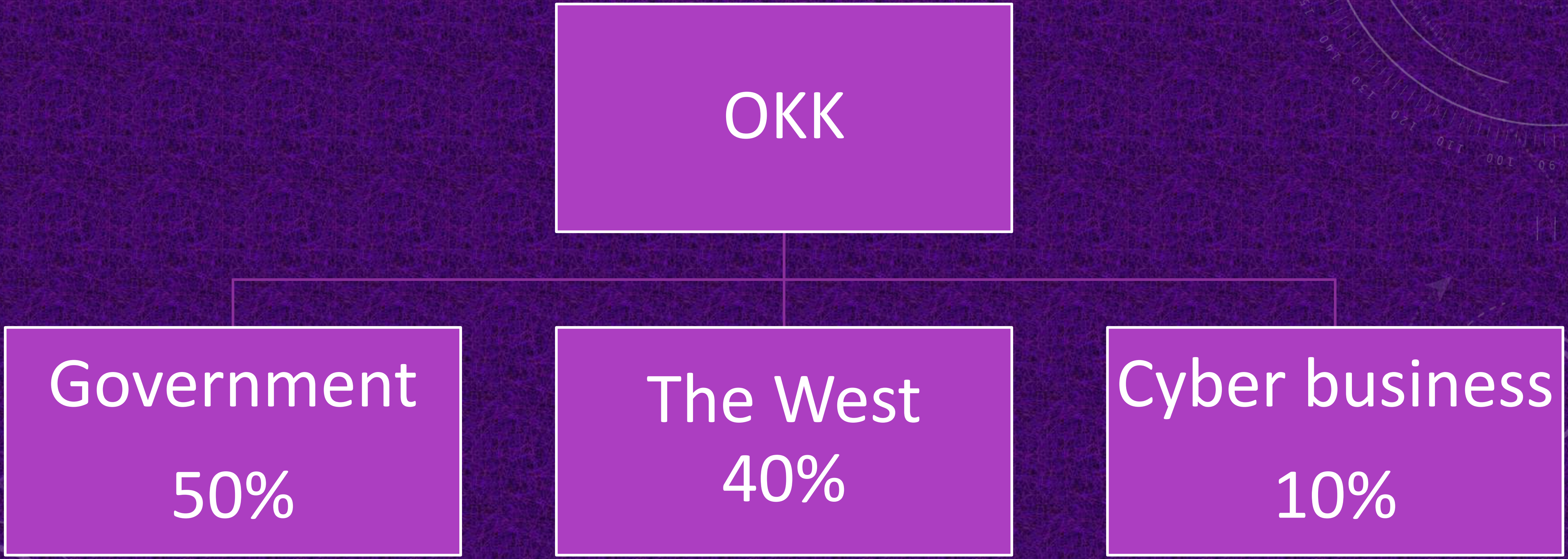
Non-profit organization

Government

The West (donors)

Cyber business (UA)

THE MATTER



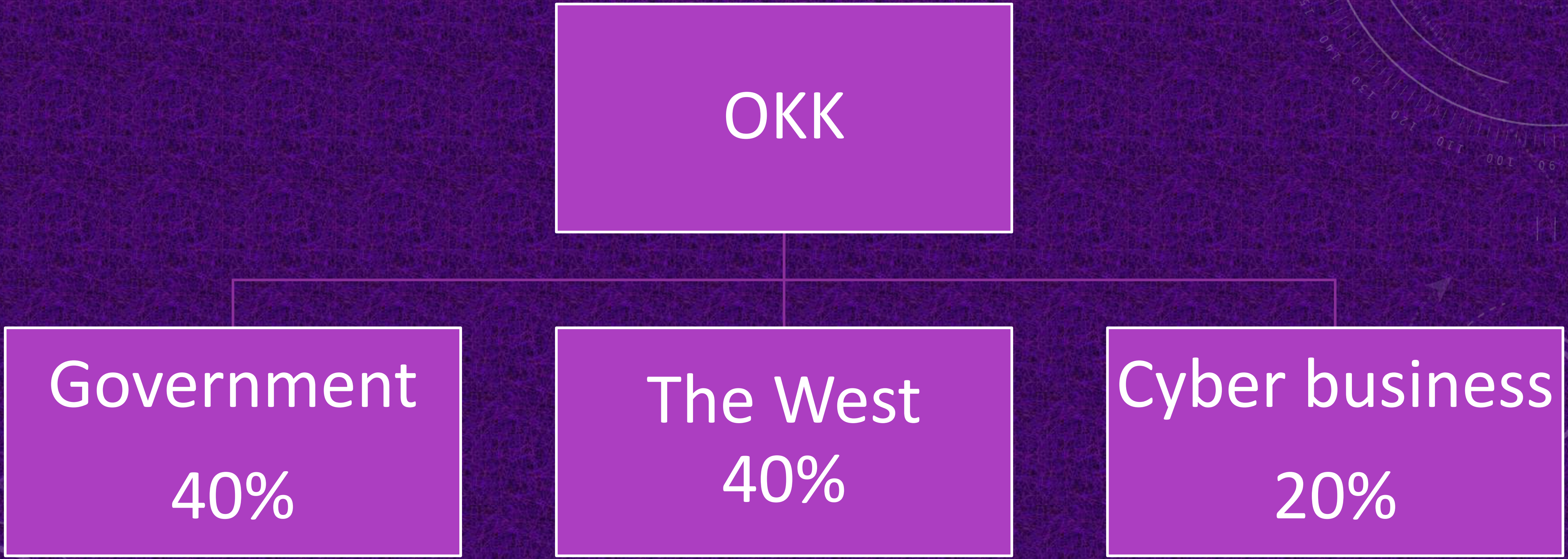
OKK

Government 50%

The West 40%

Cyber business 10%

THE MATTER



OKK

Government

40%

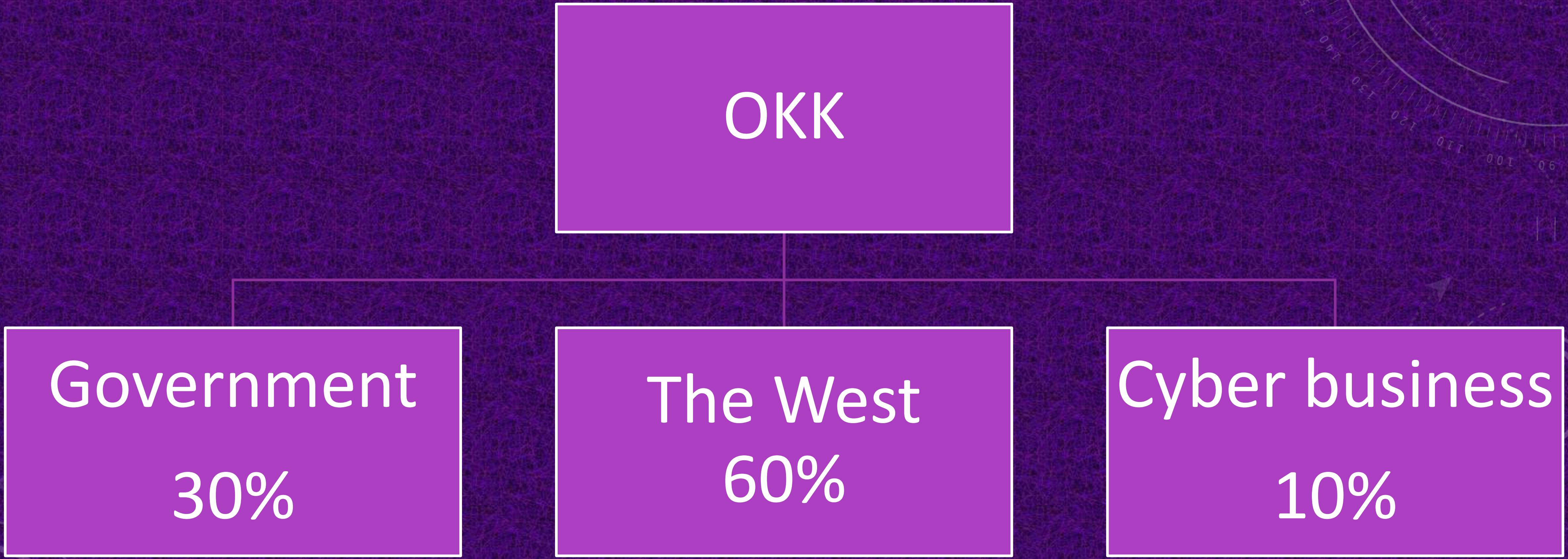
The West

40%

Cyber business

20%

THE MATTER



OKK

Government

30%

The West

60%

Cyber business

10%

THE MATTER

Why non-profit organization?

To avoid one more ‘State Agency’: corruption, improper money spending

Zero profitability: no problem what to do with a profit

Costs: only salaries, taxes, rent office, equipment, advertising, etc.

No one can earn on the problem

THE MATTER

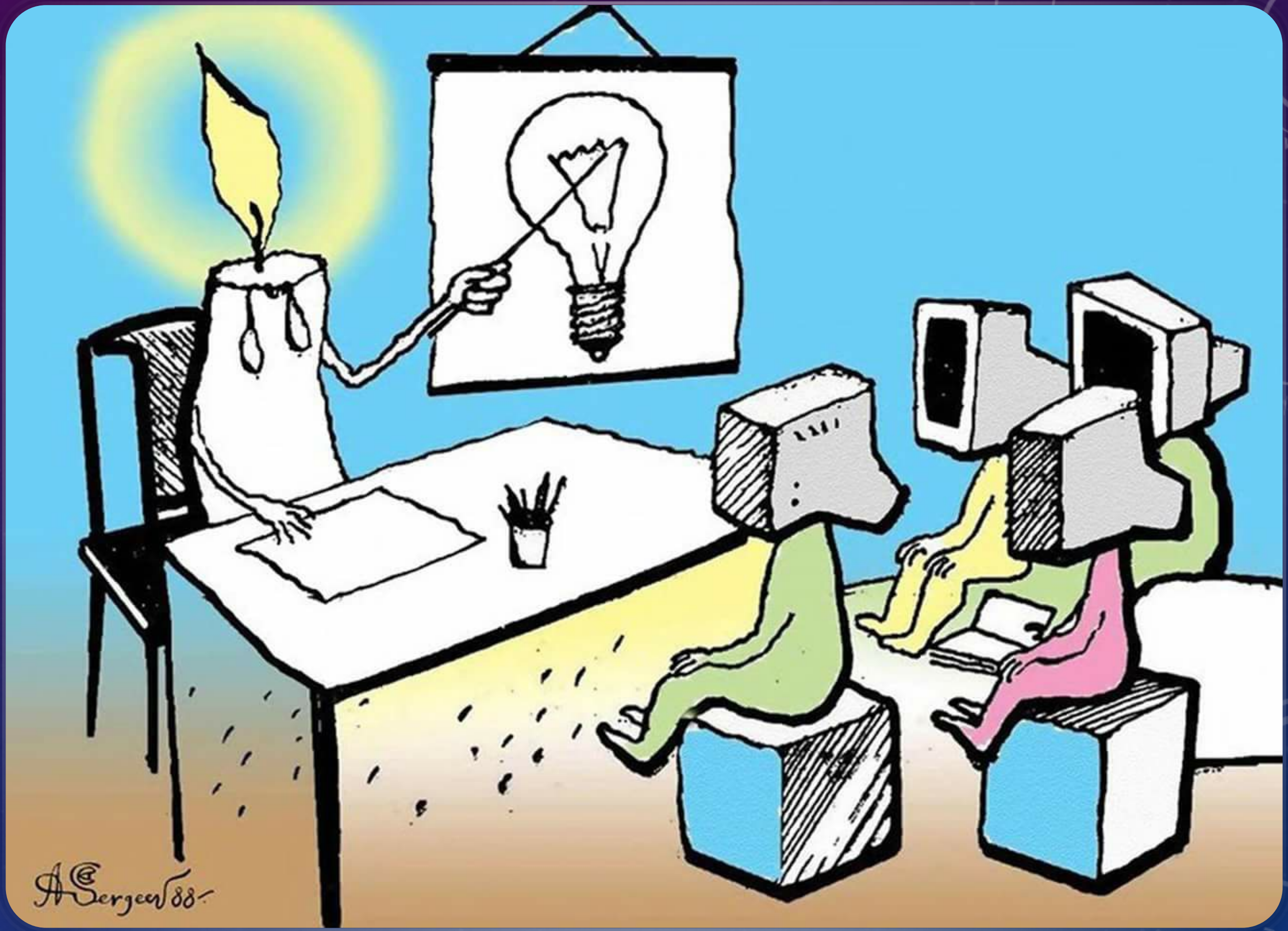
Why the Government?

Most stable element: always alive

Always has a budget

Provides national legal regulations

Point of entrance for international support



THE MATTER

Why the West?

Money

Technologies

Practical experience

THE MATTER

Why Cyber Business?

Best experts

Professional approach

Cutting-edge technologies, solutions, equipment

Readiness to cooperate

Understanding of perspectives

WHAT OKK SHOULD DO?

Free consulting: by phone, email, messengers, on-site (exclusively)

Customers: any Ukrainian resident, company, organization, public body, LE…

Cyber hygiene: massive attack via media, banners, city-lights, leaflets,in social media, webinars, podcasts, on Maidan, Tinder….

Attack’s targets: bookkeepers, doctors, students, teachers, drivers, housewives, traders, officials, waiters, *Tinker-Tailor-Soldier-Spy* ……….

Range: from ‘don’t click shit’ and ‘update AV’ till DLP, SIEM, Threat Intelligence

WHAT OKK SHOULD DO?

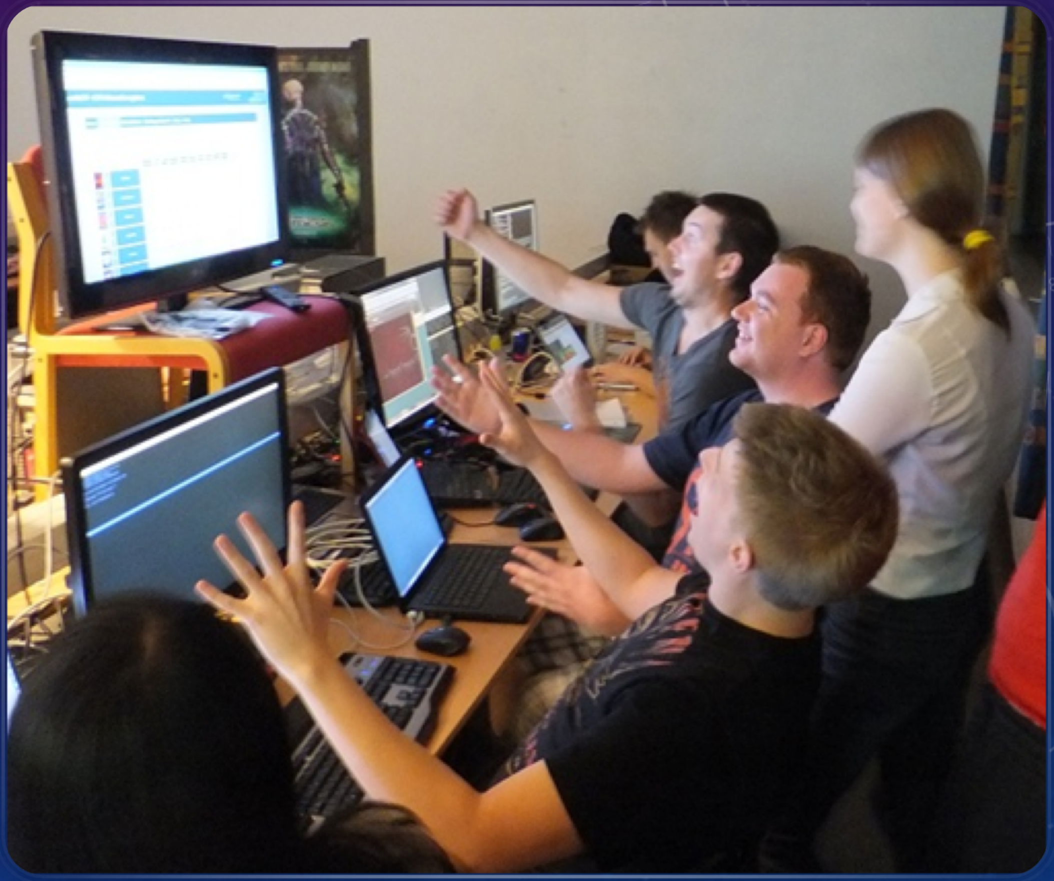
Regular host for local cyber events (like OWASP meetup, for free)

Regular host for CTF and other competitions, regular students (?) training center

News, announcements, alerts, articles, notifications, recommendations, etc. (3-4 a day)

Free consulting on cyber legislation to public authorities

To become a ‘point of trust’



HOW OKK SHOULD WORK?

Launching team:

Team Lead, ~$7k/month

Deputy/Practice unit lead, ~$5k /month

Security Officer, ~$3k /month

5 engineers, ~$2.2-2.5k /month

3 analysts, ~$2k /month

PR-manager, ~$1.5k /month

Bookkeeper + HR: ~$1k /month

Call Centre Operator: ~$800 /month

FIRST STAGE BUDGET

First 12 months budget: $920,000
+ 30% as a Positive risk buffer: **$966,000**

- Salaries & taxes = $56,000/month

- Insurance, gym, sell phone: $10,000/year

- Rent office, Internet, facilities, cleaning, water, coffee, etc. : ~$5,000 /month

- Cloud infrastructure, laptops, software & hardware, telephony, office equipment & stationery, etc.: ~$50,000/one-time

- PR: adds in Internet, media, social media, arranging public events (meetups, seminars, webinars, streams, trainings), producing podcasts, video instructions, participating in conferences, panels, etc.: $10,000/month

- Team trainings: ~30,000/year

FIRST STAGE BUDGET

One million dollars: how much is that?

- State Service of Special Communication and Information Protection budget-2019: **~$125 million**
- U-LEAD project: **~6 million EUR** already spent
- US Government is going to fund **~$10 million**
- UA Government granted **~$3 million** next day after attacks against State Treasury (December 2016)

SECOND STAGE: 2.1

Mandatory conditions:

- Successful First Stage only
- Proven mutual trusted point of contact status for business, society, professional community, and Government

2nd Stage Main Direction: incident information sharing. Origins.

Contributors: OKK's customers from 1st Stage who are interested in.

Very carefully, diplomatic treatment on base of strong and transparent rules

SECOND STAGE: 2.2

- To increase number of participants/contributors
- Expansion of cooperation with other Response Teams, CERTs, SOCs, Cyber Centers, FIRST, Trusted Introducer, …
- Additional budget: business trips including abroad, about $30,000-40,000/year

SECOND STAGE: 2.3

Thinking on

Increase/decrease e number of engineers, operators, analysts?

Hiring additional narrow-focused experts?

Get rid of unclaimed functions?

New claimed vectors? Reverse engineering, forensic, threat intelligence, training programs?

TOTAL BUDGET

36 months budget: ~$2.8 million

Including Positive risk buffer: **~$3,6 million**

- SSSCIP budget-2019: ~$125 million
- U-LEAD project: ~6 million EUR already spent
- US Government is going to fund ~$10 million in 2019
- UA Government granted ~$3 million next day after attacks against State Treasury (December 2016)

BENEFITS: GOVERNMENT

- Cyber hygiene breakthrough
- Restored trust to Government
- PPP
- Horizontal connections
- Society consolidation
- Cyber legislation level up
- Actual statistics

BENEFITS: DONORS

- Much more effective support
- Actual info on up-to-dated threats, attacks’ methods and techniques, countermeasures
- To make Ukraine successful in cyber

BENEFITS: CYBER BUSINESS

- Positive image
- Activity on the market
- Internal marketplace structuring
- Loyal cyber infrastructure would be attractive for moving SOC-teams to UA
- Recommendations from OKK to contact definite one of private co-founder

CONCLUSIONS

Yes: **start from scratch**

Yes: **begin with a small, grow fast, think on a great**

Yes: **dissociate from ineffective, incompetence and outdated authorities**

5 main principles:

1. Current System can not be fixed
2. Current System should not be destroyed
3. New System should be built in parallel
4. People is our All
5. Trust is the main goal

CONCLUSIONS

Disclaimer

the Plan wouldn’t work in case of:

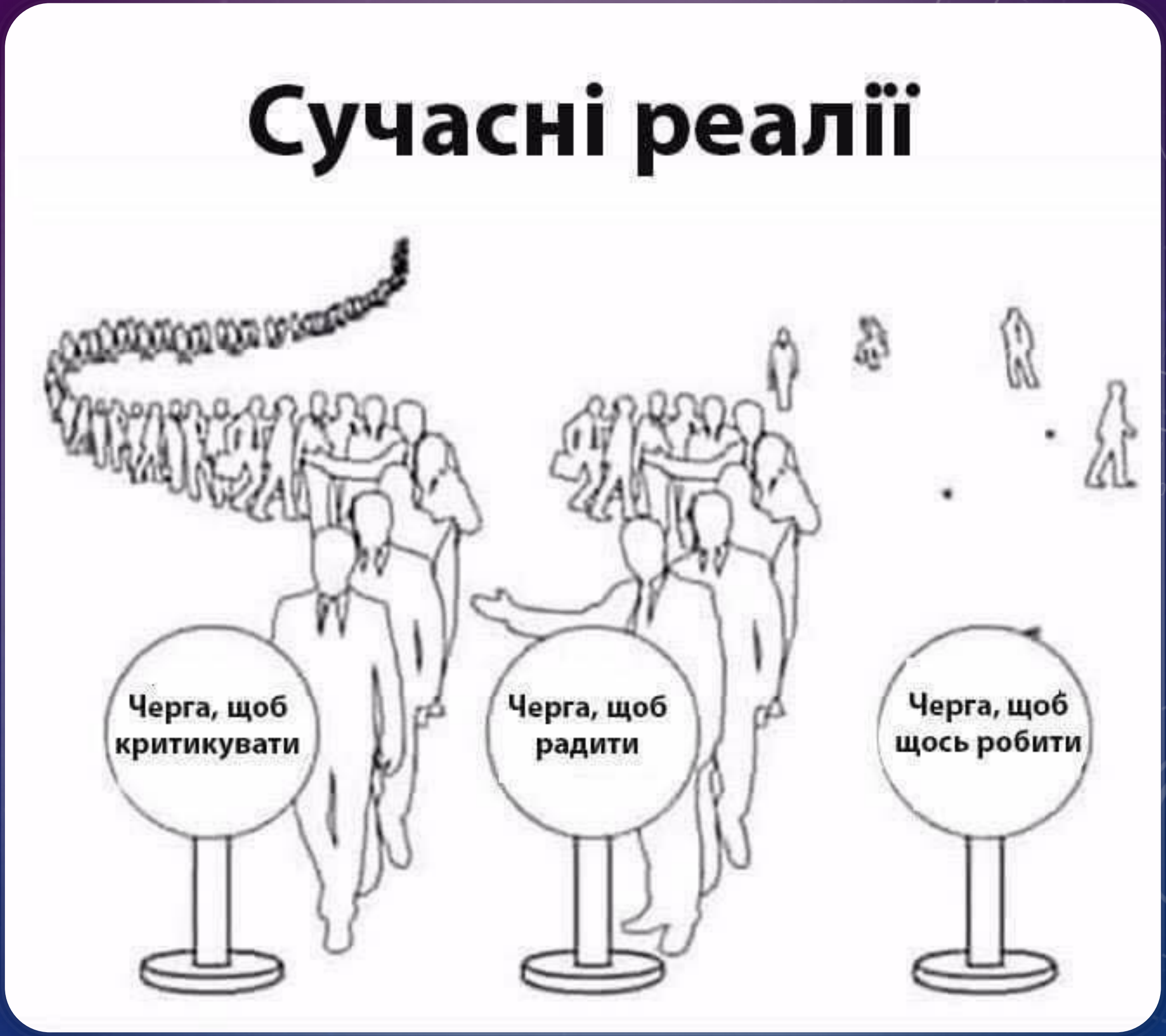
- Improper people
- Changing/ignoring key points of the Plan
- Using the Plan for stealing money/corruption/pollical influence

CONCLUSIONS

The Plan is executable

All you need: a desire to obtain a result

Professional approach, joint efforts, passion



QUESTIONS?

Where have I been worked:

- Berezha Security, co-founder and CEO (since 2014-now)
- NGO UISG, Head of Council (since 2012 – now)
- World-Known-Big-Corporation, Threat Intelligence Official Vendor (2014-2017)
- iSIGHT Partners Ukraine, international US-based cybersecurity firm (now is a part of FireEye), Director (2010-2014)
- Founder and first Head of CERT-UA (2005-2009)
- Security Service of Ukraine, e-crime Division (2000-2005)