

# Taransvar Cyber Security

## Table of Contents

Taransvar Security.....	1
Conceptual description.....	2
History of global cyber security.....	2
Consequences.....	3
About Taransvar and mental health.....	4
The task.....	5
Taransvar Advisory Board.....	5
Cyber Security Core System.....	5
Distributed cyber attack prevention.....	6
How to connect.....	7
Investment opportunity.....	8
Certification for partners and clients.....	8
Spin off products and projects.....	8

## Taransvar Security

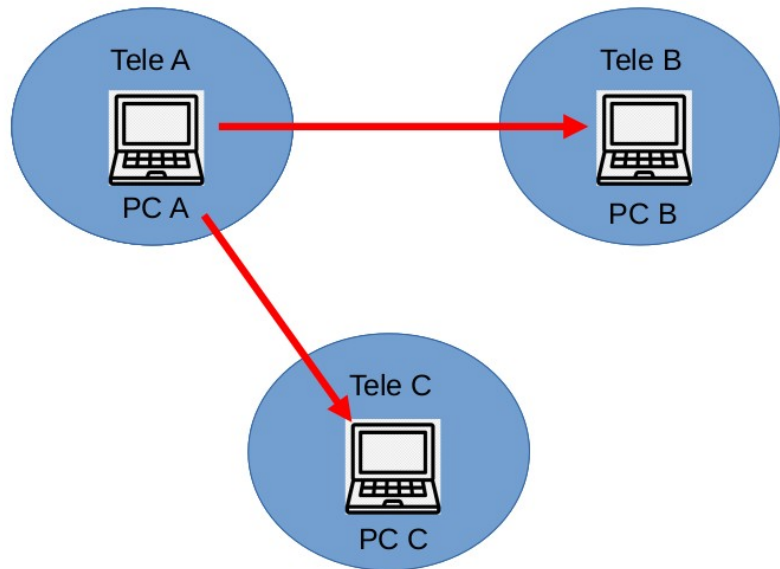
Taransvar is a Norwegian NGO dealing with mental health and cyber security for now. “taransvar” or “tar ansvar” means “taking the responsibility” in Norwegian. After some years of “thinking”, we are now in the process of launching our global cyber security concept based from Nairobi. The vision is to manage global cyber security from Nairobi. This may sound like a mental disorder, which may be why we also got involved in mental health. Jokes aside: Cyber experts confirm that if cyber security is done our way, then cyber crime will more or less go extinct because we deny them what they need to thrive: Telecom companies letting them keep on building their botnets for years without any consequences. Partnering telecom companies will handle their net as it should have been implementing decades ago. As we all understand, this can’t be done by an NGO alone. However, we think we can make it very profitable for those who contribute. So for now we’re trying to find such people in Nairobi.

Cyber crime is a growing global problem costing the global society hundreds or billion USD annually. This could “easily” be rectified if the purpose was to solve the problem and not just profiting from it. This document explains how. We “humbly” suggest ourselves as the owners of such global secured network and are dedicated to making this a success. Below is a description of such network, how we’re planning to bring this about and how you can become part of this.

## Conceptual description

It works like this:

- PC A is an infected computer in the network of telecom company “Tele A”.
- PC A is used in an attempt to attack PC B belonging to Tele B.
- The traffic is identified as an attempt to hack by PC B’s firewall.
- The firewall informs Tele A that it has been attacked by PC A
- PC A is then used in an attempt to attack PC C
- Tele A wraps all traffic from PC A in a data package informing that this computer has been reported by others to be involved in attacks.



## History of global cyber security

There is no doubt that there should be a global secured net. It has been tried before:

- America Online may have been the first attempt.
- IBM AS-400 was also an attempt to make a global secured network. But that fell with the growth of PCs.
- Microsoft NET was the next one. They came after Internet had matured enough to make it realistic. But nobody wanted Microsoft to “own” global security.

So why should anybody support Taransvar to do this job? There are a few organizations that could do the job. However, those IT corporations that would suffer financially from such net are probably so well invested there that they can easily prevent it from happening.

We think you should let us give it a try. And at the same time watch carefully how we’re doing it. If we don’t handle this in a good way, then a better alternative will emerge.

This document is explaining the full technology. Will someone steal it? We think it’s great if they try. We will claim it’s stolen and they will probably end up helping us. But that is up to our customers.

# Consequences

Getting this implemented will be a big task. Gaining accept from the market will be an even bigger. But having a multiple billion USD market is normally a good foundation for generating good business. Our concept does it the smart way: The sending telecom company know who owns the infected computer and the receiver knows with 99.9% probability if it's legitimate traffic or not. The way it is being done today seems to be tailored to maximize the profit of the IT security industry without any care for the victims.

So what are the consequences if we are able to make this a global success?

- Once a computer is identified as infected, it can no longer be used to attack computers belonging to partnering telecom companies
- Hackers will spend most of their energy on staying undetected and hacking will no longer be sustainable and will more or less stop.
- The value provided by partnering telecom companies will increase significantly and make "all" internet users who are interested in a safe connection switch to them.
- This will increase the pressure on non-partnering telecom companies and make the serious players join us.
- Those who lose will be criminals and IT security companies (they currently earn billions on the misery of others instead of implementing what's best for their customers)
- DOS attacks will also no longer be possible because companies can easily dismiss all traffic coming from infected computers. This can be handled automatically by telecom companies for servers that report abnormal traffic or too high load to us.
- Currently, telecom companies are reluctant to do "packet sniffing" because it's risky to start blocking traffic. By handling it our way, there's no spying or blocking of traffic and no other risk for telecom companies. They're just telling what others told them. You may say we introduce gossiping, which is awkward but in this case effective.
- There's great opportunities for making this profitable for a whole range of partnering technologies. Those who don't partner may be left with scraps.
- All liberal societies are moving more and more to online solutions. This means that online security will (or at least should) be a major concern. This is especially true for countries that are new to this and have sparse resources. We are solving this. Meaning that societies can embrace this change.
- Cloud computing has seen huge growth. One concern with cloud computing is that you lock yourself to one provider with proprietary technology. If we gain trust as provider of online security, then we can tap into this market, either directly or with one or more selected partners. It is unclear what consequences our concept will have for this market isolated.
- IP version 4 is very limited and the world should shift to IP version 6. Introduction of our secured network is likely to boost this transition. This will further enhance the security because we can report back to the network owner which computer in the network is infected (only the owner will know which computer it is).
- Our network will have huge consequences for how nations do cyber defense and war – which we would like to discuss further.
- This is an opportunity to introduce a global digital ID (including global secure login). This will be good for digital users but not so good for oppressive regimes - probably.
- Currently, the strategy of the IT industry is not on solving problems, but rather as profiteering on people's misery. By shifting to solving problems, we can also start

addressing problems like unsecured WiFi networks and infected private computers and provide the best tools for free as long as that also benefits our goal of making Internet secured. This may include free anti virus tools and encapsulating traffic from unsecured WiFi devices and warning the owner when there's communication with infected unit or attempt to hack other units in the network. Honey pots should also be implemented in all networks to expose threats and make hacking units in the secured network unsustainable.

- This is just a start. It's a "shift of paradigm". There will be new ideas in the years to follow.
- There are organized crime actors involved in cyber crime that is also involved in other kinds of crime. Profit is re-invested in more advanced breach technology to stay ahead of their victims. Profit from cyber crime is also re-invested in human trafficking, drugs, it boosts corrupt regimes and other crimes that cause a lot of damage. Removing the profit from cyber would help on all of this.
- We will generate many new IT jobs. This is a good combination with our work on mental health because poverty and lack of hope is a major reason for mental health problems.

## About Taransvar and mental health

Our brain has strong functions for "helping" us maintain focus. But when our focus turns dark or distracted from what we should do, then those very same functions easily become our biggest problem and may turn into any mental problem, lack of social skills or other challenges.

One similarity between mental health and computer systems is that it's at the same time very simple and very complex. Based on the basics of remembering, adding and comparing digits, you can build the most complex computer system. Based on very simple logical functions in our brain, we can build all variations of human personalities. We think that the basics in our brain is brain connections (axons and dendrites) and the connections between them (the synapses). Axons and dendrites can be considered permanent (skills, habits, personality, knowledge, trauma, mental disorders) while the synapses are what we know as getting rusty, warmed up, mood swings, sleepy, drunk and everything else that may change rapidly. And then there's the focus, which of course is extremely important though scientists seem to have little clues about what it is. We think there's nothing in our brain that supports that the basic mental diagnoses should be treated as diseases or sickness. It all boils down to maintaining a good focus over time and handling our traumas and bad triggers in a good way. That can be done by good practicing and support.

We think the solution to mental problems is to establish trust and proper coaching based on a team working together to solve our problems and find peace of mind and better ways to react to triggers. The best therapists are champions who have overcome their own mental problems and can motivate others to do the same. Our vision is to build what we call "wellness sanctuaries" all over the world. By mixing mental health with solving cyber security challenges, we can also generate lots of high quality jobs that give hope and income for many poor families – and of course a better focus.

As you may understand, getting this properly tested has been an uphill experience, so for now, we're focusing on cyber security. If you're a psychiatrist, you may not support this, but others should understand that a lot should be done when it comes to mental health. Too many get lost because they don't get proper help shifting their focus.

## The task

For implementing our global system for securing Internet, we need partners who see the value of a secured Internet and are willing to be part of the team and get their name engraved in history. We're looking for IT security, telecom companies, big corporations, governments and universities.

Hopefully the HQ will be in Nairobi, Kenya with branches elsewhere. So if you have a view on this, then you should contribute. We especially challenge those located in Nairobi to position themselves on the right side of history. Cyber crime is an ever escalating problem that costs corporations hundreds of billion USD every year. The big paradox is that it can easily be solved if there's good will to do what's best for our customers and not just what brings most cash in short term.

What are we looking for:

- Technical assistance in developing core systems for telecom companies to secure Internet
- Financial assistance in exchange for good name branding and a seat at the table
- Any other advice or assistance is also appreciated. Please also tell us if we're wrong. Then we can focus elsewhere.
- If you're willing to look for the above, then you're also welcome – especially if you also want to do something for mental health.

## Taransvar Advisory Board

Taransvar does not have any cyber security skills and is planning to govern this network through local branches and advisory boards all over the world where we're hoping to have representatives from universities, government and big corporations. As time goes by, the role may change, but in the start, it will also have to do a lot of the work on the ground.

We're starting in Nairobi, Kenya, but we also want to have such advisory boards elsewhere. So we are looking for people who are willing and able to connect us with universities, telecom companies, government and big corporations to make this also happen in other countries. Those who contribute will be compensated as soon as there's income in the specific country.

## Cyber Security Core System

We are developing an open source system (maybe to be closed later) that:

- Connects those who knows what is legitimate traffic (the receiving firewall) with those who know who sent it (the routers of the sending telecom company). This is the key to good cyber security though it was never implemented.
- Tags traffic between partnering telecom companies and other key partners
- Lets the receiving end know when they might want to block traffic and does the job for them if they want. This way, our customers are not only protected by their own firewalls but by all other connected firewalls and telecom companies. This is of course bad news for providers of firewalls and criminals but very good for everybody else.

The system currently runs on (Ubuntu) Linux and has four main components:

- A kernel module c-program that acts as part of the operating system and receives notification about any traffic that is sent through the system and also does the tagging and blocking.
- A “link” modules c-program that connects the kernel module with a database and a front-end “dashboard” for configuration and monitoring.
- Primarily perl scripts that run in the background and monitor the system.
- A central database that collaborates with the local installations to provide the best setup and governance. This is just in the earliest stages but lots of effort will be put in this.
- Soon also more firewall and “honeypot” functionality on the router.

Doesn't this exist in the market already?

Modern routers and firewalls have advanced features for inter-communication and encapsulation. There is even a collaboration between the biggest firewall providers sharing white- and blacklists (and thus locking out the smaller providers and forcing you to buy a very expensive one).

So if you buy one of those expensive routers, you may get something like this. However by locking out the other providers, they miss intelligence from all those who are not willing to be part of their exclusive “club” – and that's where most of the threat is. And it leaves the exclusive club members to guess if it's ok or not based on IP address and port – which is a very bad solution compared to collaborating with the telecom companies.

Tagging challenges

One central point in the system is tagging or encapsulation of presumed malicious traffic. This is currently handled by using a less used field in the TCP header, which is the “urg\_ptr” field. This field is intended for situations where a part of the datapackage is more urgent than the rest, and thus should be transferred first. We're lacking knowledge here, but this seems a bit odd because the layers of the OSI model ensures that the whole package is transmitted before it's handled over to the applications. So the actual usage of this is unclear except from the fact that there's still lots of traffic passing through the network where this field is used. When we're testing, we experience both that traffic is let through unchanged, that the urg\_ptr field is set to 0 and that tagged traffic is being blocked. And it seems like it's domestic wifi routers that are most notorious when it comes to blocking such traffic. So we need to find a good way to handle this in collaboration with routing hardware providers or others.

## Distributed cyber attack prevention

The first project we're planning to release is addressing what we think is the biggest challenge online

- Brute force attack is when hackers are using thousands of infected computers in a botnet to guess passwords
- 
- D-Dos (Distributed Denial Of Service) attack is when a botnet is used to overwhelm a server and render it unavailable (denied ability to deliver their services)
- Spoofing is when hackers forge their sender IP address to conceal their true identity, normally in email or "DNS amplification attack" (not sure if that's still an issue) because those protocols do not require “handshaking”.

The cost of this inflicted on the global society is hundreds of billion USD annually and it can easily be eradicated using our methods.

For the first two categories, the solution is to send messages to notify partner routers that a specific IP:port does not want any traffic from presumed infected units (can specify classification) when server load exceed a specific level. This can easily be automated.

The last problem is that ISPs let "spoofed" (forged sender IP or email address) traffic into the network. The reason why they do that may vary:

- There may be valid routing reasons to do so and it's very risky for ISPs to block such traffic
- They don't care enough implement routines to stop it.
- They're somehow involve in the crime

If the receiver request them to block such traffic, then blocking it is not risky. So that is the solution.

Our challenge is that most ISPs will be reluctant to implement such measures unless we give them good reason to do so. We can do that either directly or through their customers or by creating awareness and demand from governments or the market in general. According to "Akamai" (I don't know who they are), "bots compose 42% of overall web traffic; nearly two-thirds are malicious". That should be enough reason for telecom companies to support our project.

Development requirement

Our system is not yet ready to be deployed, but our demo system is ready for testing.

Implications for ISPs


ISPs can implement this either by integrating our "Gatekeeper software" into their main system or by moving presumed infected units to a separate segment that is guarded by our system. Choosing the last solution has some consequences. If there's overload in their system, they can easily switch off this part of their network and save the important customers. They can also prioritize traffic. Being able to block traffic without risk is in their interest. And getting rid of the garbage traffic should be in their interest.

## How to connect

For now, our main communication channels are:

- The Facebook group page "[Mental health awareness and solutions](#)" (click the link to join)
- A whatsapp group called "[Global Cyber Security](#)" (click the link to join)

The core team - we are all on Whatsapp:

<p>Wanna get your face here?</p>	 <p>Damaris Nkatha Sales and marketing +254 724 272 232</p>	 <p>Øystein Torsås Research and development. +47 99647892</p>	<p>Wanna get your face here?</p>
----------------------------------	--	---	----------------------------------

## Investment opportunity

Taransvar is a non-profit organization. We don't have the capital to develop and launch this in an optimal way. So we are looking for financial partners who are willing to avail the necessary capital in exchange for a fair share of the future profit. Please contact us if you have any suggestion on this.

## Certification for partners and clients

To prevent abuse, there must be a system for certification in place for those implementing the Taransvar routers and also for any entity to receive encapsulated traffic.

Requirements for telecom companies:

- Unique (anonymous) identification of presumed infected units
- Maintaining the system, communication lines and similar
- Prevention of spoofing

Requirements for other entities:

- Confidentiality
- We should not give this to just anybody. Reason why they need it should be given and also requirements for size, reputation and other operational criteria.

## Spin off products and projects

If we succeed, there will be many spin off products in the years to come. Those who help us get this properly started will not regret if we succeed.