# The modern form of knowledge growth

## The enlightenment

## Forum for information security

is the basis of any espionage.

Because they can be successful only there, where is the knowledge that they want to acquire. Thus, your first task begins to successfully to knowledge to get, what they want to obtain.

The number of this "knowledge" is tremendously high in the kybenetischen area. Select only, where is the knowledge of them.
Also hierzun there are a number of methods that come from the classic spying. It should be not entered on them, because she would be beyond the specificity of the cybernetic space. It however is very important to the information from the back to access.
In many cases, open sources are a very interesting note. Because they know Yes, loud Putin come **100% of the information or knowledge from Open Sources. This man must Yes know it.**

You need to transform only this knowledge into the cybernetic space. What is no different, they need to identify the targets of their hunger for knowledge,. The comparison with the PIN in a haystack is appropriate here, however, the relationship between haystack a PIN is much higher, because they have to do it with a "global network".
So have fun in the search.

But, perhaps, this search is not yet so large?

Try to optimize it using the "search engines".

The result is a small mountain of possible destination addresses now. The emphasis is "possible" on the formulation, they know even how careless to deal with "Keywords".

Before they take further steps, they need to evaluate this destination addresses. What expectations do you the knowledge you want of them containing the destination address they have chosen?

Since the "classic intelligence services" have it easier.

Now they have a manageable mountain on destination addresses, which they believe it contains their "missing knowledge that they need to expand through espionage.."

## Countermeasures:

**They liquidate all information related to sensitive information of your company in the cybernetic space (all the information that create added**

**value for them are the) on the "kraken", another name for the "search engine", for a good uses system that operates in this case the opposite. ) Is only about the information that they have put themselves in the global information system in this case.**
**You yourself have published this information!**

## The target analysis

Before them, the remote attacker, a mountain is located on destination addresses of possible targets.

Now comes the phase of the destination that you would like to wasting Spionagemittel Yes not for nothing, even if some do it. What resources there are used depends in General on a number of factors, "classic method" may be this, as well as an attack from the cybernetic space, or also combined actions are possible. For this, it is amazing what knowledge you would expect. At the same time, also the safety standard plays a role with which they protect your information (knowledge). This phase is the time of the analyst, it must establish are what destination addresses to "investigate" as a priority and which have a lower priority.

At this stage, they are condemned as a possible target for the inaction. You feel like "the rabbit before the Snake", you must wait if the information is "valuable" within the meaning of the requirements of the contracting authority, which aims to achieve an increase in knowledge.

At this stage be no activities which can be recognized, whether or not they are a target.

### Countermeasures: no
### You feel like "the rabbit before the Snake",

## The methods for the penetration of the target object

If the decision failed to penetrate the target object, not still know whether they belong to or not. You still feel "the rabbit before the Snake". But they do not withstand this state of affairs, either them together or they break lernes it with this State to live.

They have however, long lived with this condition, why expire them now in this hustle and bustle? Oh well, their information is Milliiarden US $ worth. For the "proper recipients" much more than the billions of them referred to their knowledge with this, earn.

The value of their information and thus the related knowledge, should also significantly smaller than the above sum it enough to feel like before a snake.

Now they need to worry yet "".

What problem is the "possible spy" for now?

This is the crucial question, where it does not clearly answer can he selects the "Classic method" or the "cybernetic"method or but a mix of both variants.

1. the classical method
This method is then gewäht when "menschlikche sources" in the target object already exists.
While the "classic form" of intelligence can be applied...Another way is through a direct attack on the cybernetic unit of the target object without using the cybernetic room by the existing human sources. **Points of action - man- (the input) or Output channels)**

2. the cybernetic method
If there are already detailed information about the cybernetic unit of the target object, ensure the a targeted and successful attack of the Spionagemittel.
If this information is not available, is by an upstream attack, investigate the target object.
These attacks take place directly from the cybernetic space using the resources of the cybernetic unit. **(Point of attack - the online communication to cybernetic space)**

3. the mix - method
This method is as the name implies is a mix of classic and modern.
The attack is carried out on the cybernetic space (cyberspace) with or without support of the human capacities available in the destination GPO. The "gained knowledge" will be sent by cybernetic space to the customer.

The attack is carried out on the cybernetic space (cyberspace) with or without support of the human capacities available in the destination GPO. The "gained knowledge" is sent by the human sources to the customer.

The attack is carried out with support of the human capacities available in the destination GPO. The "gained knowledge" will be sent by cybernetic space to the customer.

## Countermeasures:
## Have they taken all necessary protective measures?
## If not, it could be now already too late!
## Are their protective measures adapted to the value of information? Pay attention urgently to's attack points

### The gathering of information

They will not experience unfortunately this event, or unless, the "burglar" have gone badly.

The term "Burglar" was chosen deliberately because they know can be classic burglar or staff of their companies; but also "cybernetic arrows" can it with their highly intelligent spectrum around to get to their molds; or act as well as to the combination of both methods.
So can it pazieren the the "burglar" several times their "Haunt cybernetic unit." Rather than

because he has forgotten what no, because he has taken everything still on the first burglary.
This second slump he used the same way as the first time, because they have to this day still no idea which one their cybernetic unit or had several days of "open door".
To catch the "burglar" red-handed, they must increase as your security level that meets the requirements of modern safety requirements. They already know their weaknesses, so you know what they should do urgently. They analyze the value of their information - or in other words - the increase of knowledge for the customer of the burglar. It should nevertheless to time delayed damage your company come and they would have to log on to the end of bankruptcy, then they have at one point decide "wrong traded".
They have been wrong in one place, they have their "Competitors inexcusably underestimated." He now makes their profit!

The temporal classification of information gathering, they are basically according to derZielplanung and the initiation of the operation for the production of information. Whenever it starts the attacker to determine when it ends, is determined by various factors:
-the necessary time to "go out all the relevant information";
-other important information are discovered during the analysis which require an extension of the operation;
-the operation will continue in time intervals, because this is from the information analysis;
-the analysis of de security measures revealed no changes to the information already available;
-the operation object does not have the information you want; Incorrect operation
-the amount of interesting information has already been reversed, any new information in low yield of target object - target blank
-no structured information found; faulty analysis of the target object
-Blocked access to databases; faulty analysis of the target object
-no access to the information faulty analysis of the target object

The success of "break" for the purpose of "free knowledge mining" depends on the quality of information on the target object.

If they see a slump after the "classic method", by an "employee" or you can it call other ways, they are in very good company. A "qualified employees" has stolen several gigabytes or more, from a network of security of the US Government. About the damage, said Government authority for the information security of Government information is silent.

**Countermeasures:**
**Protect all information about their cybernetic unit. Thus, you complicate the chance of success upon entry. Brag with their security systems. Because there are always people who show them that their security system is yet "Holey".**
Continued!

000

Berlin, 11 / 2011

Old Gocs

**Original:**

Es soll auf diese nicht eingegangen werden, Da sie die Spezifik des kybernetischen Raumes sprengen würde.