SA WEST Global intelligence

Russian private intelligence agency

Corporate Security Program Assessment

COUNTERINTELLIGENCE ASPECT

Foreword

Since ancient times the idea of security is based on the so-called “perimeter concept”.

Valuable assets, tangible or intangible, for security reasons, must be localized somewhere inside (or outside) the perimeter and properly monitored.

All instruments of security are based on attempts to keep most valuable assets inside a protected perimeter.

Extrapolating this idea, security professionals tend to make the perimeter as big as possible and protect it with the most advanced methods and technologies.

But what if the perimeter concept is not as solid as it seems?

Challenging The Perimeter Concept

The first challenge to the perimeter concept was related to the data. For many years information and data seemed to be a kind of golden coin that we can close in a safe, monitor and protect.

The same time, considering the data as intangible asset, business expects that the data will generate profit, will “move”, but will not leak. This contradiction between security and business tasks triggered discussion about the nature of security in the modern world. Security is important but profit is the highest priority for the business.

Since mass introduction of cloud technologies, the fact that the border between inside and outside data of the corporation/individual does not really exist is widely discussed by IT community and data protection specialists.

In XXI century we see that there’s no chance but to accept the fact that we can’t border all valuable assets and must learn how to live in more complex environment. Old school security methods are under pressure in most industries.

Introducing Intelligence

Corporate security is aimed at protecting the assets of the company mostly on site or in the semi-public domain. Unfortunately, the business of the company exists in a much wider context. The ability to work within this wider context distinguishes intelligence agencies from other less resourceful aggressors. Not mentioning all types of state databases, databases of mobile operators, banking records etc. – these sources are hard to access in certain jurisdictions – there're unobvious means and methods of obtaining sensitive data on the company with a comparatively soft approaches. We have to admit that in the overwhelming majority of cases, intelligence agencies use all these methods without proper monitoring and countering by corporate security.

Another issue requiring attention is that corporate security management often suspended from control over classified or sensitive activities of the company. Top-management and shareholders used to operate voluntary, make up their own minds what to believe and what security procedures to follow (or not). This practice makes some critical data of the company absolutely unprotected from local and foreign intelligence agencies.

Introducing Intelligence

Long before it was publicly declared that the Perimeter Concept can't cover all issues of the modern world, intelligence and scientific entities successfully developed the methodology of datamining the Subject without penetration of the perimeter or even the Subject's knowledge.

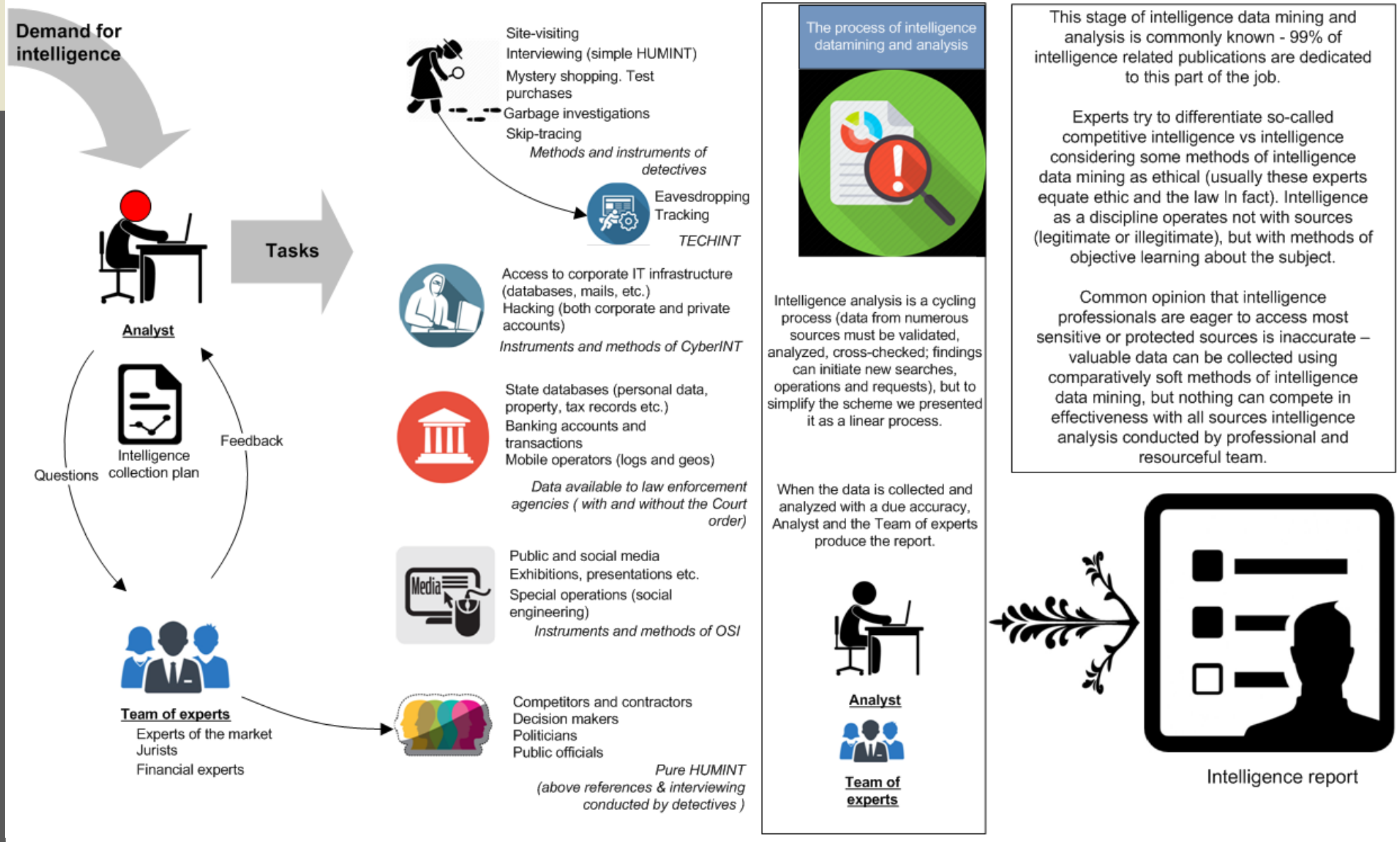
In the XXI century the global trend of using foreign intelligence services and specialized private agencies against companies and individuals is increasing:

- The frontier between business interests of global corporations and politicals have become blurred. That's why some political tasks can be assigned to private agencies and at the same time every governmental intelligence agency works for private corporations.
- In the private sector there're several commonly known players in the intelligence market and a large number of small and mid-sized specialized agencies working in certain fields (markets, regions, issues, types of intelligence etc.). Most reputable private agencies are headed by ex-officers with remarkable records of achievements and strong links to domestic and global governmental entities.
- It has become a common practice recent years to assign foreign agency (governmental or private) to solve local issues if the task is not in compliance with local regulations or the Client wishes to avoid possible leakage of the information to law enforcements of his native country.

How It Really Works.

Stage 1 – intelligence datamining and analysis

Only 10% of intelligence demands are about stealing secrets and/or industrial espionage.
40% - support of decision making process
45% - influence subject's activity and decision making
5% - uncommon tasks and operations

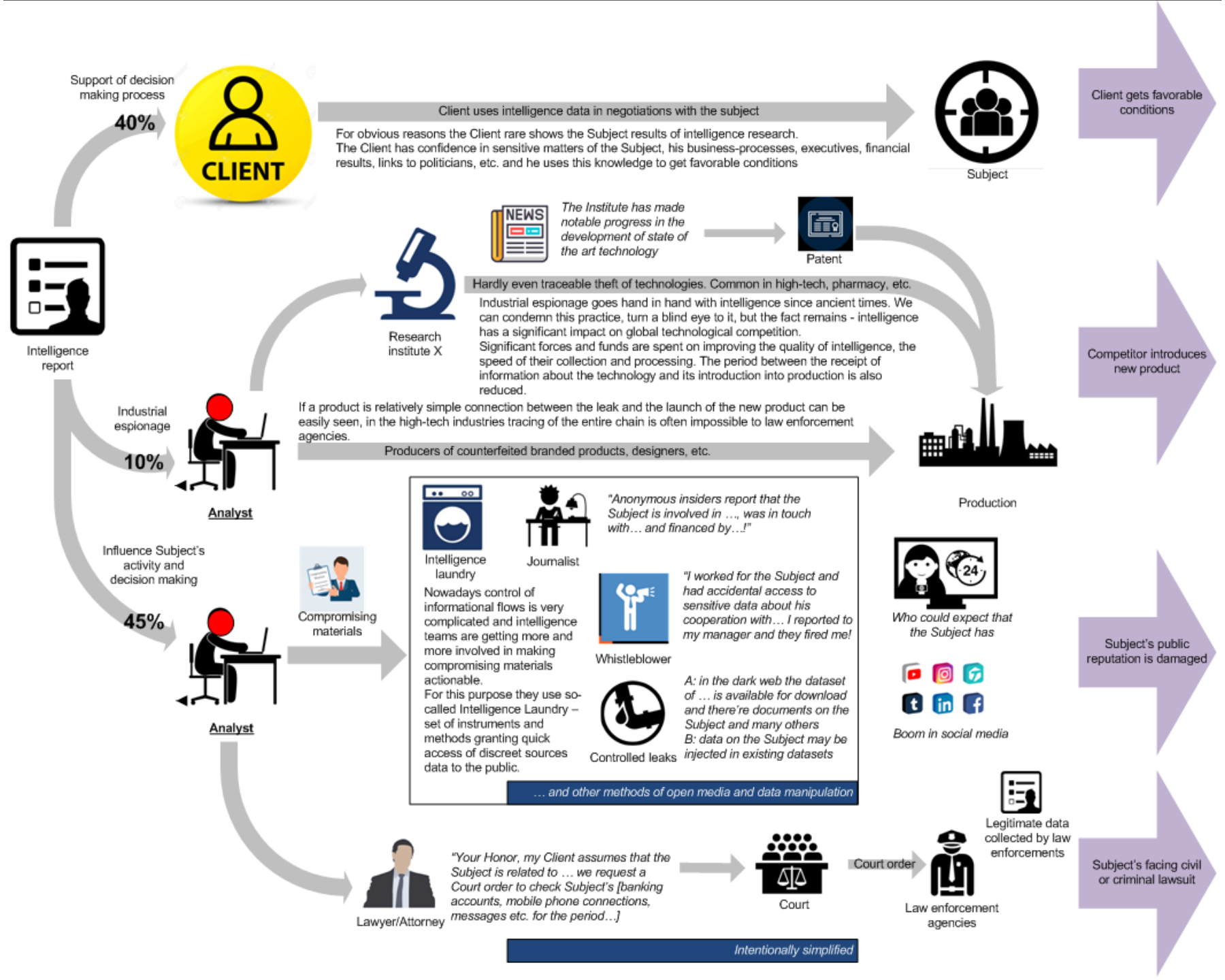


How It Really Works.

Stage 2 – making intelligence actionable

When the team has successfully collected and duly analyzed intelligence data on the subject it's time to make intelligence actionable.

There're many different strategies and some of them don't require expertise of the team [the Client takes the process under direct control], but in recent years intelligence teams are getting more and more involved in Stage 2 activities.



And what's on the surface?

Many companies and private investors (Subjects) see results of Stage 2:

- Partner unexpectedly got favorable conditions [in negotiations, in M&A deal, in lobbing of state contracts etc.]
- Competitor introduced new product
- Negative media coverage seriously damages Subject's reputation
- law enforcement agencies unexpectedly aware of the most intricate deals and connections of the Subject

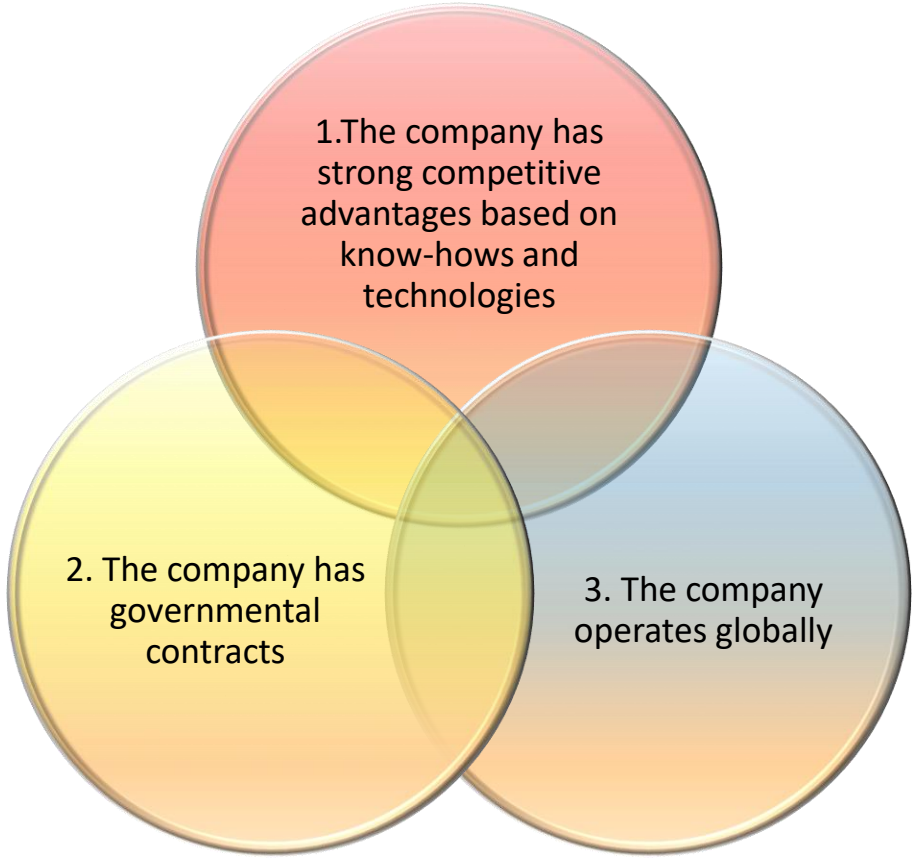
but it is unlikely that the Subject will consider these hardships as consequences of intelligence activity.

Who Must Be First Forewarned?

Three groups of companies are under the constant threat of collisions with intelligence agencies:

1. A company with strong competitive advantages based on experience, operating globally and working with governmental contracts would be 100% in focus of intelligence agencies.
2. If only two of the above statements are true, this probability is above 60%.
3. For some companies it is enough to be a global operator or develop a unique technology or have industry experience to become subjects of intelligence operations.

Obvious targets for intelligence agencies are companies and corporations involved in projects of geopolitical significance, defense companies and military contractors



Counterintelligence

The discipline helping corporations to deal with intelligence entities is called Counterintelligence.

Counterintelligence activities shall be undertaken to detect, identify, assess, exploit, and counter or neutralize the intelligence collection efforts, other intelligence activities of foreign powers, organizations, or persons directed against the corporation, its personnel, information, materials, facilities and activities.

The problem is that depending on the origin and culture of the attacker different procedures and methods of counterintelligence must be developed for effective protection of the company.

Some basic approaches are common, but most important and critical tasks of counterintelligence are unique and require practical knowledge of methods and schemes used by agencies of different origin.

Counterintelligence overview

Good old days approaches:

A. Let's put "confidential" seal on every document, check all employees using polygraph to find the rat, keep communication under control (mail, phones, internet traffic etc.), require authorization for every personal contact etc.

Counterintelligence in this context is considered as a security discipline ["we must protect …. against intelligence activities of foreign and local powers"].

B. Our main task is to gather intelligence on intelligence entities, know what they do, what they plan to do, how they collect information; we must know their main targets and way of thinking. Also we do our best searching for agents operating on the ground.

In this context Counterintelligence is a part of intelligence.

In fact it was a very comfortable approach: CI doesn't need any specific methodology, intelligence officer can be transferred to counterintelligence department without long-term training.

Up until now counterintelligence is a function of intelligence agencies of many countries, so this approach proved to be effective.

Counterintelligence overview

Modern approach:

You can’t ensure 100% protection of data. Every known fact can be uncovered with the appropriate budget and effort, so you must try making the price of accessing this data too high for intelligence teams. Since the 1970s, ideas of risk-management were dominating the market and counterintelligence disciplines were also seen from a risk-management perspective. This approach was a remarkable step forward for Counterintelligence.

From an academic point of view, the methodology of counterintelligence has always been less developed in comparison to that of Intelligence. The first systematic attempts to consider counterintelligence as a unique discipline [not as a brunch of Security or Intelligence] brought a lot of valuable methodological findings, initiated appropriate research and brought about reforms in most of the world’s professional units.

Using this approach the corporation should first estimate the price the aggressor will have to pay for accessing sources with sensitive data on corporation’s activity – this task can be solved by corporate security manager or assigned to the third party, no matter.

Then it is reasonable to ensure that easily accessible sources don’t contain critical data on the company or the data in these sources is manipulated in a manner that will disinform the aggressor.

Finally, when the company understands that supposed aggressor will have to pay an awful lot to get to the data of real value, the system must be regularly checked and tuned.

This approach has many advantages for big enterprises because it can be documented, standardized and adjusted to the corporate security program. The main weakness of this method is in its common implementation. Making intelligence collection plan some aggressors can easily predict what types of sources the corporation is keeping under control.

Counterintelligence overview

Millennial approach:

In many spheres, attempts to counter intelligence activities of foreign and local entities proved to be too expensive, ineffective and even disruptive.

Counterintelligence must be targeted on solving two main issues:

A: Disallow any understanding of current actions of the Client. Sending of numerous dubious signals is more effective in comparison to total silence or disinformation.

B: Intelligence and Counterintelligence don't exist without the concept of time. Both are targeted on the future [*compare with investigations – we can trace and investigate only footprints of the past, but Intelligence is about future steps by the Subject and our ability to predict and counter these steps*]. To solve counterintelligence issues, we mustn't just consider making some facts unavailable (incomprehensible) to the intelligence entity, but we should ensure that the Client will have time to make his actions BEFORE the intelligence entity will be able to gather intelligence and predict the Client's future steps.

The rest must be focused on security, intelligence and public relations.

Conclusion

1. Counterintelligence and security are solving different issues.
2. Security is responsible for protection of assets INSIDE the perimeter and this task is critical for safety and peaceful development of every individual, corporation or even state.
3. Considering counterintelligence as a supplementary discipline to security is a dangerous mistake.
4. Security shouldn’t be harmed for successful attempts of intelligence datamining and obviously for consequences of the fact that someone made intelligence actionable.

The same time, some elements of security program if analyzed and considered properly, can seriously support counterintelligence function and bring much value to the business.

For a free copy of a brief security program assessment check-list (counterintelligence aspect) get in touch with Dmitry Ivanov of **SA WEST Global Intelligence**
dmitry.ivanov@backgroundscreeninginrussia.com

Make sure that your security program has sufficient flexibility to respond to new challenges coming from inside and outside of the perimeter.

www.sawest.eu