

Cybercom

# Counter Intelligence Services – CIS

Counter Intelligence Services (CIS) delivers strategically important information about your company's exposure to illegal or unethical methods of competition driven by organized crime, governments or competitors.

**Counter Intelligence Services (CIS) delivers strategically important information about your company's exposure to illegal or unethical methods of competition driven by organized crime, governments or competitors. No antivirus, firewall or product solution will adequately handle the problem of industrial espionage for you because the adversary will not hesitate to break the law, manipulate individuals and is often well financed. The result of CIS levels the playing field and gives our customers a competitive advantage and the necessary tools to handle this threat effectively in a tough market.**

### We watch your back

Almost all IT-Security focuses on preventing the vaguely defined threat of external intrusion by a low level entity. This might be a realistic threat scenario for the average small business, but for businesses that drive the market and business of scale such a threat scenario will leave you with nasty surprises.

A serious intrusion often involves one or more of the following: insider involvement, bugging, customized malware, conmen, fake job interviews, radio transmitters, personnel manipulation etc.

The Nordic Forensic Team is a world leading task force that helps you detect attempts to steal and manipulate your most valuable information and protect it before its too late. We are seasoned investigators of industrial espionage and international fraud cases. Based on years of experience we know where to look and what look for and provide you with a flexible intelligence organization to counter serious threats before the damage is done.

### How we operate

Industrial Espionage and crimes against the company is always a top management issue, therefore we primarily deal with company management when setting up our operational structure and handling cases. There is also the ongoing problem with insider involvement in many severe cases which makes us want to minimize the amount of people inside the organization that knows about our presence.

At the first seating after business formalities are cleared away like confidentiality agreements, billing arrangements and involved personnel a workshop is held that aims at answering the following:



What significant values exist in well documented formats that provide or will provide the company with a competitive advantage? The answer to this question will guide us in what type of setup will be the most appropriate and efficient in handling the possible threats and misuse of this information and countering the most probable ways it might be extracted or manipulated.

What dynamic values with less documentation exists or are in ongoing processes in the organization like: significant orders, strategic investments, large contract negotiations, etc. The answer to this question will guide us in determining if there are significant risks of this information being wiretapped, bugged, or leaked and how to identify if that is the case and how to counteract.

The answers to these questions are an ongoing process and demands different counter intelligence solutions at different times. However, some information and management of that information is more stable and makes it possible to implement more

permanent ways of supervision. Solutions include dedicated logging and tracing equipment, information traps, cryptographic solutions, pre crime intelligence collection from external sources, personal or company background checks etc.

In addition to the more permanent solutions above specific situations might require more adaptable and improvised solutions for dynamic value protection such as: bug sweeping, undercover opponent interviews, screening of other entities, information planting, disinformation schemes etc.

### Conclusion

If you are a market leader or a big business that holds research information, strategic business information, or any other competitive or deal information that will provide significant revenue in the future you will have to handle the threat of industrial espionage and related crimes. No antivirus, firewall or product solution will adequately handle the problem of industrial espionage for you because the adversary will not hesitate to break the law, manipulate individuals and is often well financed. What you need is Counter Intelligence Services that adapts to the situation and protects what is really valuable.

- To counter a malware – use a product.
- To counter industrial espionage – use an organization.

### About Cybercom

The Cybercom Group is a high-tech consultancy that offers global sourcing for end-to-end solutions.

The Group established itself as a world-class supplier in these segments: security, portal solutions, mobile services, and embedded systems.

Thanks to its extensive industry and operations experience, Cybercom can offer strategic and technological expertise to these markets: telecom, industry, media, public sector, retail, and banking and financial services.

The Group employs 2000 persons and runs projects worldwide. Cybercom has 24 offices in 10 countries. Since 1999, Cybercom's share has been quoted on the NASDAQ OMX Nordic Exchange. The company was launched in 1995.



### Contact Details

For further information, please contact:

Emil Nordström; Head of IT-Forensic Services  
*emil.nordstrom@cybercomgroup.com*  
 +46 70 356 67 57

Tomas Rimming; Business Area Manager  
*tomas.rimming@cybercomgroup.com*  
 +46 8 726 77 65

[www.cybercomgroup.com](http://www.cybercomgroup.com)