Information Warfare in the Corporate Business Environment

by Dr. Giselher Dombach, Jens Greiner and Maxim Worcester

War is not an intellectual activity but a brutal physical one. War always tends towards attrition, which is a competition in inflicting and bearing bloodshed, and the nearer attrition approaches to the extreme, the less thought counts. Nevertheless, few who make war at any level seek to win by attrition, all hope for success at lesser cost. Intelligence can help reduce the cost by identifying weaknesses in the enemy`s method of making war or in his systems of defence. Examples for this in the past was the breaking of the German codes in 1940 which gave the British crucial intelligence. The success was as much breaking the codes as was the fact that the Germans did not know that their traffic was being read. This in turn led to the British, and later the Americans, planting disinformation which further weakened their enemy.

In the last resort, intelligence or information warfare is a weak form of attack on the enemy. Knowledge is power, but knowledge alone cannot destroy, deflect or defy an offensive by an enemy unless the possession of intelligence and knowledge is also allied to force. Intelligence is important, but it is a secondary factor in war. Intelligence can only work through strength.

Many of the concepts of Information Warfare in the military context can be found in the world of business. In the corporate context, Information Warfare is often associated with Industrial or Economic Espionage and Cyber Crime. Counterintelligence as practiced by the Military is known as Information Protection in the corporate world. Disinformation is practised both by the Military to confuse their enemy and by companies to influence their customers and discredit their competitors. There are many similarities between the ways in which the Military and the corporate world work; they do so however for different reasons. In the case of the Military, Information Warfare is used to conduct attrition in a manner which will lead to maximum harm to the enemy at minimal cost to the own side. In truth, it is about brutal, physical conflict which ends at best in surrender, at worst in death. Companies do not seek to follow this path, they employ Information Warfare to maximise margins and market share and to dominate and control markets. Ryan Air, an aggressive and successful airline might declare war on its arch rivals British Airways and Lufthansa; it will however not seek to shoot down its rivals aircraft. The vocabulary might be the same, but not the methods in which Information Warfare is put into effect.

These differences need to be taken into account when one looks at the use of Information Warfare in the corporate business environment. The thoughtless use of military terms in a civilian environment can damage the reputation of companies, especially when such terms are used in countries where the Military has a low standing and the use of force is rejected. The use of words such as “Wirtschaftskrieg” (Business Warfare) in countries such as Germany is

counterproductive. Such companies are likely to be blacklisted by clients and potential clients, thus rather defeating the purpose. Private Equity companies made this mistake in Germany some time ago, their aggressive manner of doing business earned them the reputation of behaving like locusts as they asset stripped their way through the country. To this day such companies are referred to as “Heuschrecken” (locusts) in the press.

Companies do well to use Information Warfare as a part of their strategy. They must, however, be very clear in their external communication that Information Warfare in the world of commerce is very different from Information Warfare as practiced by the Military. The words are the same, the execution however not.

Business as a Battlefield

The borders between economic and military battlefields have become increasingly blurred. Military doctrines of Information Operations are used by competitors and stakeholder opinions are influenced by means of distributing and communicating selected information. The reputation of companies is damaged using strategic leaks to the press and to persons of influence.

When the Swedish energy company Vattenfall launched its campaign “Climate Signature” in 2008 in various media, including its web site klimaunterschrift.vattenfall.de, it did not anticipate the reaction of its arch enemy Greenpeace. It countered the campaign with a smart and effective campaign of its own by acquiring the domain klimaunterschrift-vattenfall.de. The difference between the dot in Vattenfall’s website and the minus in that of Greenpeace was spectacular. The Greenpeace site was confusingly similar to that of Vattenfall, but very different in content. It exposed Vattenfalls campaign to be nothing more than a case of “Greenwashing” and made the company look ridiculous. Vattenfall was sloppy in not reserving for its own use all possible sites which had a similar name, thus exposing itself to an effectively organised counterattack.

Such attacks are not new; they are however on the increase due to the increased use of the Internet and lessons learned from the use of disinformation by the Military. As the Military ramps up the use of Information Warfare, more people are trained in this field. Eventually they leave the Military to claim well paid jobs in Industry where their talents are of great use. Increasingly lies, unproven statements, rumours and the full repertoire of psychological and cognitive actions are used to attack the corporate enemy. Such Mind Bomb attacks are not replacing the classic instruments of marketing, in some companies, however, they are running a very close second to the classical methods.

The effective use of web 2.0 has added a further set of weapons. The use of all interactive media such as blogs, twitter, social media and other tools helps agile (and usually small) companies in their fight with the unwieldy (and usually large) companies or even Governments. Campaigning is thus no longer a battle of budgets but of creative minds and innovative methods. In many ways this has a similarity with asymmetric warfare. Mastering the channels of web 2.0 has become a decisive factor in the war of reputation, both in the business world and in the field of politics. Simply placing a rumour in an important blog can initiate a campaign which can easily unfold further without any further input from the initiator. A clip strategically placed on You Tube can result in the creation of a dedicated website, comments on Twitter and even coverage on TV. Greenpeace is good at this.

Such activities, however, can backfire. In 2009 Verizon attacked AT&T on its poor 3G coverage. AT&T counter attacked with the offer of an open debate on its own Facebook site in an honest attempt to turn the argument in its direction. The result was less than helpful for AT&T as the majority of the responses were in fact critical of AT&T. These criticisms were on the AT&T site for all to see.

This case illustrates the need for a rapid and well thought out response using the most effective range of communication methods. Speed and the use of the right response are crucial. The longer an accusation remains uncommented, the more credibility it is given. This does not mean that speed of response is everything, it is speed and content which is decisive. Companies need to have suitably trained people ready not only to respond but also to anticipate any such attack. AT&T was aware of its poor 3G coverage; it should have expected an attack and should have prepared its response in advance. It is well known that one should not formulate a defence strategy when under attack; such work must be done in advance. If weaknesses are known and identified before they become apparent to the competition, information can be planted in suitable media which blunts any attack of a competitor. In the case of AT&T they could have simply let it be known that the problem was known and that steps were being taken to rectify the situation. Such a move would have placated the customers and taken the first mover advantage away from Verizon. The attack would have been aborted by Verizon.

From a military point of view information is not only bit and bites. Information is gathered to gain an advantage over ones adversary and is integrated in operations. Information Operations (IO) and Information Warfare (IW) are comprehensively defined in doctrines manuals and concepts. Within the context of Fourth Generation Warfare, operating with information disciplines is crucial to realise effects.

The following definition of IW is helpful in putting this into the civilian context:

"*Information warfare (IW) is an embracing concept that brings to bear all the sources of a nation-state or business organization in a coherent and synchronized manner to control the information environment and to attain and maintain a competitive advantage, gain power and influence. […] IW occurs when, in the physical and virtual domains, you attack your competition or they attack you. IW is about synchronized and coherent relationships and capabilities.*"[1]

These definitions illustrate that we are confronted with a wide aspect of tools around the concept of information. They include a range of technological tools and the ability to use these in the most effective manner. It is the latter which is the most significant in the successful use of information. Influencing decisions, spreading disinformation, protecting information and mystifying achievements cannot be undertaken without being smart and alert. The tools need to be available; the winner is the one who uses them best, not the one who has the best tools.

Reputation as a Soft Target

Managing reputation is not easy at the best of times, during a crisis it becomes an art. Crisis managers need to evaluate reputational risk factors and concrete threats and need to be able to respond rapidly with well thought and much practiced plans. Too many companies spend time

[1] Global Information Warfare – How Businesses, Governments, and Others Achieve Objectives and Attain Competitive Advantages. (Andy Jones, Gerald L. Kovacich, Perry G. Luzwick), 2002, S. 28

only on formulating plans and not enough time on practising and fine tuning such plans. When the time comes to put such plans into effect, most those involved in the response have never sat around the same table.

Reputation is considered to be an intangible asset and it is difficult to measure the monetary value. Reputation can be considered to be a part of the psychological and cognitive domain and is thus a soft target. Other corporate values such as people, information, capital and goods can be protected with physical means; reputation however cannot be thus protected. The true value of reputation becomes clear when the reputation of a company or a person comes under attack. The undermining of a companies reputation can lead to the loss of market share, a falling stock price or the loss of contracts. Stakeholders loose the confidence in the company and the leadership. In the case of the workforce this can result in key managers leaving the company to join forces with the competition.

Attacks on corporate reputation are only a matter for crisis teams in the last resort. Prevention of such attacks start much earlier with issues management, an early warning system designed to identify possible attacks on a company's reputation well in advance. Issue management discovers, identifies and evaluates the potential impact of any such attacks and seeks to instigate changes within the company which mitigate the risk of attacks on the reputation of a company.

An example of such an attack was the case of a small but successful company which came under pressure from a group of hostile stakeholders. The company came under increasing attack from this group through the use of chat rooms and also openly during the Annual General Meeting. The stakeholders openly criticised senior management, accusing them of being incompetent, lazy and lacking an equity story. Top management time was wasted in a number of ineffective meetings which did little to help mitigate the threat. Such a response is frequently observed when no crisis plan is in place and can at best be described as "muddling through". Eventually the company appointed an executive to set up an issues management and crisis management team in order to counter the attacks from the stakeholders and to prepare the company professionally for future attacks. Had such a position been in place from the outset, the attack could have been nipped in the bud and damage averted from the company. For the company in question this mission was expensive both in financial terms and in reputational loss.

The Brent Spar case in 1995 is an illustration of how expensive reputational loss can be and how best to counter attacks on the reputation of a company. When the owners of Brent Spar, an oil storage facility in the North Sea, decided to sink the structure in the ocean rather than scrap it on land, Greenpeace opened a vigorous attack on Shell. Greenpeace deliberately inflated the amount of oil which was still in the storage facility, claiming that it still contained 5500 tons of crude oil. Shell countered with the figure of 75 – 100 tons. Months later Greenpeace withdrew its claims, confirming Shells numbers. But the damage had been done. Thousands of motorists in Germany boycotted Shell petrol stations and the company spent large sums of money in regaining its reputation. Brent Spar was towed to Norway to be scrapped, a move considered by environmentalists subsequently as grossly exaggerated and unnecessary. There is a second part to this story, however. Brent Spar was used not only by Shell but also Esso. At the time this was never reported, nor was Esso ever in the focus of Greenpeace. The company had a superior crisis and issues management structure in place and was able to defend itself effectively from Greenpeace. To this day most people who remember the event remember Shell and Greenpeace, but not Esso.

Such attacks on the reputation of a company can be direct or indirect. They can also be either overt or covert and can come in the form of a massive attack or a series of pin prick attacks.

The corporate world can learn from the Military in identifying and countering such attacks by studying methods, techniques and procedures of the military intelligence cycle. In a military context intelligence is not only a branch of the Armed Forces, it is also the description of a product and a process. The product is known as actionable knowledge, process can be described as systematic steps with clear activities. It is in short a clearly defined way of thinking and acting which is understood by all concerned.

For an organisation under attack it is of utmost importance to understand what is really going on and who is the enemy. Furthermore it is important to know who ones natural allies are and who is the person or organisation pulling the strings behind the scene. A company in such a situation needs to rapidly asses the expected reaction of the stakeholders and formulate the appropriate strategy. Intelligence in the military sense thus is of crucial value to prevent and solve problems and crises. The use of human intelligence (HUMINT) or open source intelligence (OSINT) can be used to profile stakeholders and provide actionable intelligence. HUMINT in the military sense involves the use of espionage, an option not open to corporations, at least legally. In the corporate world HUMINT is simply establishing and maintaining a network of contacts who are in the position of providing intelligence. OSINT is a much undervalued method of using available published sources in order to track what the competition or stakeholders are undertaking. Such tracking is an effective early warning tool which results in the corporation having the time to develop a response to a future threat.

Stakeholder intelligence is becoming ever more important as the use of blogs, internet, social networks and web 2.0 make the dissemination of information and disinformation easier and faster. This becomes especially true at times of new product launches or mergers and acquisitions. In such times companies are in the focus of stakeholders and are susceptible to attacks from the competition and those critical of the company. In such times companies need to be especially vigilant and need to keep a close watch on unfolding attacks.

The Military have an advantage in this over corporations as they continuously practice and act as if they are under attack. Much time is spent in exercising and on manoeuvres; they are trained to expect an attack at any time. The corporate world concentrates on conducting business, making money and growing market share. An attack is therefore an unusual situation, unlike the Military who are trained to expect an attack. Increasing competition between corporations, the use of both legal and illegal methods of conducting business and the increase in economic espionage by countries such as China and Russia call for a higher degree of awareness of the dangers which corporations face today and increasingly in the future. Corporations are well advised to look closely at how the Military conducts and counters Information Warfare.

Recommendations

Given the threats described corporations should take the following steps:

- Implement a special issue, intelligence and crisis management unit reporting to the CEO
- Activate intelligence procedures as a central way of thinking and acting
- Install an early warning and reconnaissance system
- Develop networks which can be of use when under attack

- Develop methods to identify and profile relevant stakeholders
- Use communication strategies and tactics to counter any attack on the corporation
- Test the effectiveness of all methods employed on a regular basis and fine tune methodology for maximum effectiveness.

Information Warfare has become a part of daily corporate business reality. Corporations need to be aware of this fact and are increasingly required both to counter attacks on their corporations and mount attacks in order to maximise business opportunities. The proper use of intelligence and the professional gathering of intelligence is fast becoming a strategic advantage for those who master this process. Those corporations who choose to ignore both the threat posed by Information Warfare and the opportunities this discipline offers will loose out in this new battle.

For the Military knowledge of the enemy has always been of paramount importance, modern corporations equally need to know the plans of their competitors. Corporations can learn from the Military how best to gather intelligence and how to act on the intelligence. As the great General and politician George Washington remarked:" The necessity of procuring good intelligence is apparent and need not be further argued." Most modern business leaders would agree.

***

Remarks:

Opinions expressed in this contribution are those of the authors.

Giselher Dombach

Dr. Giselher Dombach is the CEO of GEDcom AG, a competitive intelligence company headquartered in Germany and represented by an office in Cairo, Egypt. As staff officer of the reserve trained in military intelligence he served terms of duty in Kosovo and Afghanistan. His main interest is stakeholder intelligence and transferring military concepts to the business domain. He lives mainly in Cairo, Egypt.

Jens Greiner

Jens Greiner holds a university degree in management and economics. Being a freelance consultant with focus on security-, crisis- and stakeholder management, he advises and supports several crisis teams mainly of international companies. In the past he was a military officer holding various leading positions, e.g. as company commander, and instructor roles. In addition, he was specialized as a military target group analyst in providing advice on analysis of psychological approaches and communication strategies in the context of target group management.

Maxim Worcester

Maxim Worcester is Senior Advisor at ISPSW, Berlin. Before, he was Senior Manager for Advisory Forensic at KPMG International. In the past he was Managing Director of Control Risks Germany, and held senior positions at the Economist Intelligence Unit, the Frankfurter Allgemeine Zeitung and Deutsche Börse AG.