Excerpts from
Harnessing The Power of

# *Intelligence*

## *Counterintelligence & Surprise Events*

***A Proven Framework and New Tools for***

- ***Predicting Threats and Opportunities***
- ***Analyzing Stakeholders (F-Scale)***
- ***Selecting Reliable Allies and Teams***
- ***Building a Culture of Intelligence***
- ***Hitch-Hiking on Surprise Events***
- ***Mining Virtual Communities***


**Alain Paul Martin**

***Special Collaboration***
***Dr. Brian Morrissey***

Library of Congress Control Number: 2002093491

National Library of Canada Cataloguing in Publication Data
Martin, A. P. (Alain Paul)

Harnessing the power of intelligence, counterintelligence and surprise events: a proven framework and new tools for predicting threats and opportunities, analyzing stakeholders (F-Scale), selecting reliable allies and teams, building a culture of intelligence, hitch-hiking on surprise events, mining virtual communities / Alain Paul Martin

Includes bibliographical references and index.
ISBN 0-86502-924-5 (bound).—ISBN 0-86502-296-8 (pbk.)

1. Business intelligence–Management. 2. Intelligence service.
3. Psychographics. 4. Risk management. 5. Strategy. I. Title.

HD38.7.M368 2002 658.4’7 C2002-900108-0

The Professional Development Institute PDI Inc. (PDI) publishes Executive.org books. “Executive.org” and the logo on the cover with arrows pointing 45º northeast in a square are trademarks of PDI. For details, visit: www.executive.org. All trademarks are the property of their respective owners. Printed in Canada.

Published simultaneously in the United States and Canada.

Several sites provide a free forum for consumers and corporate buyers to publish and view complaints about products and services.[277] Some pay a royalty based on the frequency of access to published complaints.

Used in the counterintelligence community, *Cyberalert, Spyonit* and *Ad Facts* are free electronic search services discussed in the section titled External Sources of Business Intelligence (Chapter 5).

Finally, Leonard Fuld (cited above) offers an extensive bibliography and "webliography" of both competitive intelligence and counterintelligence services.

## 4. Counterintelligence Road Map

- Target Risks

Counterintelligence scanning must cover constituencies and other risk-prone elements scattered throughout your value chain. These constituencies comprise current and lost customers, suppliers, staff, business allies and adversaries ranging from competitors who play by the rules to the underground fanatics who don't. We will learn more about them in Chapters 9 and 10.

- 20 Practical Steps to Build Counterintelligence Throughout Your Value Chain

Ideally, counterintelligence should be embedded throughout your value chain. It means constant vigilance on the following fronts:

1. Learn about counterintelligence tools and practices. Consult the recommended web sites at the end of this book including the U.S. Secret Service : web pages titled *The Best Practices for Seizing Electronic Evidence.*[278]
2. Consult providers as well as chief intelligence officers in leading companies with an ethical track record and operating in unrelated non-competitive fields.
3. Define valuable property (physical, intellectual and virtual). Review policies for information disclosure and asset visibility. Ensure that all corporate assets, including open-source information, meet the latest policies. Systematically

document tacit knowledge and subject it to intellectual-property protection rules.

4. Identify counterintelligence targets, i.e., anyone whose vested interest is to profit from gaining non-authorized access to your physical and intellectual property or damage your standing with clients, allies, staff and other constituencies. How much do they already know about you and how did they find out? Identify the current and plausible intelligence-collection goals of the above targets. How much is the dollar value of your tacit and explicit intelligence assets worth to the adversary?
5. Define your structural vulnerabilities: How does your environment (i.e., location, industry, neighborhood, working climate) constitute a targeted and/or collateral risk? Vulnerability grows with employee dissatisfaction, inadequate communications and poor leadership. Without addressing the root causes of dissatisfaction and maintaining a positive working climate, counterintelligence activities will produce marginal results at best. Worse, they may backfire, particularly if they lack transparency or do not gain the staff's trust. Note that high standards of privacy and personal data protection are among the prerequisites to build credibility and trust.[279]
6. Identify human-resource vulnerabilities, i.e., risk-prone people in your own back yard and their potential motivation (greed, addictions or debt, past history, strange behavior). Identify the weakest points in your supply chain and customer relationships. Watch for well-trained intelligence agents who can apply for any job in your company and/or impersonate legitimate clients, suppliers or the media. These candidates do not exhibit the traits of risk-prone staff. They will work hard to blend with the community, gain the trust of their official employer or business contact and glean both explicit and tacit intelligence. Organizations that lead their industry sometimes unknowingly fall prey to these agents who operate undercover for the competition or other enemies.
7. Trace the exposure paths of your own staff, which may include work, private homes, planes, hotels and so on. Note

that valuable intelligence was recovered by Oracle from the trash of the private homes of Microsoft staff. Also travel ultra-light and always keep valuable documents and data in sight and within reach.

8. Maintain and monitor a comprehensive log of interactions between your organization and all stakeholders, including visitors to your web sites. That is how Microsoft was able to reconstruct the incubation of "denial of service" attacks that paralyzed its portals on January 25, 2001.
9. Use security-enhanced operating systems such as SE Linux that "provide a mechanism to enforce the separation of information based on confidentiality and integrity requirements. This allows threats of tampering and bypassing of application security mechanisms to be addressed and enables the confinement of damage that can be caused by malicious or flawed applications."[280]
10. Take counter-measures to detect and prevent electronic surveillance as well as unauthorized modification, destruction or substitution of your network components and information. Note that your competitors, foreign agents and intelligence brokers may find subtle ways to enter your premises and hide powerful electronic surveillance equipment in a conference room or even a bathroom. They can also legally obtain accurate satellite imagery with less than one-meter resolution to observe your installations, parking lots, loading docks and designated trucking fleets. Pictures from the IKONOS commercial satellite and Russian DK satellites are now priced for small firms and farming cooperatives.
11. Take decisive action to prevent tampering with other assets and business secrets (e.g., competitive intelligence software, data, lists, plans, tools, know-how, systems, telecom networks, web sites, practices, technology). Keep guardians or carriers of these assets safe from hostile intelligence services and other security-risk agents (e.g., people, computer worms, viruses, Trojan horses, electronic surveillance, steganography[281]). For staff members who may be requested to provide passwords under duress, provide "alternate passwords that set off alarms."[282]

12. Seed and scatter knowledge-based assets (e.g., trade intelligence, source codes, paper waste, process methodologies) over multiple secure locations and teams to reduce risk of total access, contamination or loss. The seeding exercise should meet the legal requirements for a court order to "cease and desist" should this become necessary.
13. Consider legal and ethical deterrents, tracers and means to outmaneuver, dislocate, apprehend and seek compensatory damages from offenders. Make it particularly costly for major competitors to intrude, rob company property or collude with insiders. The system should operate under cover to intercept predatory attacks while still in early incubation. Ideally, your organization should be able to extract a written cease and desist commitment without affidavits and be promptly paid compensation to keep the case away from courts.[283] As the noted French writer, François de la Rochefoucauld, once said, "it is a great ability to be able to conceal one's ability."[284]

    If you suspect unauthorized access to your data, paper waste, fax transmissions or e-mail system, seed discarded paper, fax communications and e-mails with information traps to provoke traceable action. This is how a Swiss bank found and thwarted an insider-trading scheme. The staff of a European bureau of the *Los Angeles Times* did the same when the system logs revealed access to their e-mail at times when they were absent. The culprit, a senior foreign correspondent, read the spurious e-mail sent to his coworkers by another bureau. Unaware of the sting operation, he raised bogus issues that led to his dismissal.
14. Avoid performing sensitive transactions and communications using laptops, mobile phones and palm-held tools unless they are certified as tamper-proof. In order to ensure that confidential information remains impenetrable to unauthorized parties, use reliable encryption protocols to support transactions between storage media, caches and motherboards as well as in wired or wireless communications. Consider Fortezza-compliant cards to secure your messaging system.[285]

15. Use scenario planning, simulation, brainstorming to play the devil's advocate by scripting a series of potential moves of competitors and hostile players, disgruntled ex-employees and former partners. In high stakes cases, it is often worthwhile to ask retired executives from the competition or war room strategists, experienced trial lawyers and film-makers to shadow current and emerging opponents. In our consulting practice, we have organized script-writing contests among teams of various clients to get insights into the mind of their respective competitors, both direct and indirect.

    In the 1980s, Alcan was intent on winning Ontario's $70 million market for pop cans. Alcan executives insisted on simulating not only the strategy of direct competitors such as Alcoa, Pechiney and Kaiser, but also indirect competitors such as the producers of glass, plastic and steel (Stelco and Dofasco) and even "grass-root foes" such as Pollution Probe.[286]

    Created in 1999 with a five-year grant from the U.S. Army, the Institute for Creative Technology (ICT) at the University of South California (USC) is the most advanced simulation research center "incorporating virtual humans in key roles as characters, playing the roles of friendly and hostile forces".[287] In the aftermath of September 11 attacks, "government intelligence specialists have been secretly soliciting terrorist scenarios from top Hollywood filmmakers and writers."[288]
16. Train staff and close allies to cultivate a social system dedicated to building and preserving intelligence capital. Warn everyone about the lengths to which unethical firms will go in industrial espionage, including placing bogus career ads to extract competitive intelligence from innocent applicants.
17. Keep disaster recovery and contingency plans current.
18. Hedge against residual risks.
19. Ensure that the CEO frequently stresses the vital links between excellence, intelligence security and counterintelligence. Even the Department of Energy where

security is paramount, "has appropriately emphasized excellence in the quality of its scientific and technical work, but only recently has begun to emphasize security, and only in recent months has articulated the importance of counterintelligence."[289]

20. Ascertain that counterintelligence is a worthwhile investment that is subject to continuous improvement. Conduct regular audits and vulnerability assessments to ensure adherence to the above guidelines.[290] Narrow the scope and the portfolio of assignments through continuous pruning to focus on high payoff goals. Always compare the cost of counterintelligence with the damage it seeks to prevent.

- Summary

Organizations must begin by establishing counter-intelligence policies, building awareness and hiring trustworthy people who practice prevention at work and elsewhere. Practicing intelligence security means using secure-Web technology; seeding files, printed directories and confidential documents; video-recording the constant ins and outs of working areas; enforcing counter-measures; shadowing hostile activities; benchmarking response; and embedding virtual traces and auto-dialing chips on expensive plant equipment and computer hardware. It is also important to communicate strategies that can act as a deterrent to potential risk agents.

## 5. Conclusion

Like competitive intelligence, counterintelligence is mission-critical to every organization. Both should be an integral part of its culture and fabric. In most organizations, however, few employees have any skills in competitive intelligence and much less the skills of counterintelligence. Many only act in response to surprise events, and then do so in haste. Yet, a practical knowledge of the discipline can be significant and valuable in preventing or managing risks, as the illustrations in this book suggest.

A number of our clients in the financial and high technology sectors have discovered that relying solely on the work of best experts is costly and impractical. They found the logic of

"teaching people to fish" in counterintelligence the most-effective route to leverage the time and effort of the very few experts with core competence in this domain.

## *PART TWO*
## *-*
## *INTELLIGENCE ANALYSIS AND INTERPRETATION: NEGLECTED ISSUES AND BREAKTHROUGH TOOLS*

Interest speaks all sorts of tongues,
and plays all sorts of parts, even that of disinterestedness.
**François de la Rochefoucauld**

If you know the enemy and know yourself,
you need not fear the result of a hundred battles.
If you know yourself, but not the enemy,
for every victory gained you will also suffer defeat.
If you know neither the enemy nor yourself,
you will succumb in every battle.
**Sun Tzu**