

Journal of Intelligence Studies in Business



Journal of Intelligence Studies in Business

Publication details, including instructions for authors and subscription information: <https://ojs.hh.se/index.php/JISIB/index>

Book review: *We never expected that – a corporative study of failures in national and business intelligence* by Avner Barnea

Klaus Solberg Søylen^{a,*}

^aDepartment of Engineering, Natural Sciences and Economics, Faculty of Marketing, Halmstad University, Halmstad, Sweden; *klasol@hh.se

To cite this article: Søylen, K.S (2021) Book review: *We never expected that – a corporative study of failures in national and business intelligence* by Avner Barnea. *Journal of Intelligence Studies in Business*. 11 (3) 76-79.

Issue URL: <https://ojs.hh.se/index.php/JISIB/article/view/JISIB Vol 11 Nr 3 2021>

PLEASE SCROLL DOWN FOR ARTICLE

This article is Open Access, in compliance with Strategy 2 of the 2002 Budapest Open Access Initiative, which states:

Scholars need the means to launch a new generation of journals committed to open access, and to help existing journals that elect to make the transition to open access. Because journal articles should be disseminated as widely as possible, these new journals will no longer invoke copyright to restrict access to and use of the material they publish. Instead they will use copyright and other tools to ensure permanent open access to all the articles they publish. Because price is a barrier to access, these new journals will not charge subscription or access fees, and will turn to other methods for covering their expenses. There are many alternative sources of funds for this purpose, including the foundations and governments that fund research, the universities and laboratories that employ researchers, endowments set up by discipline or institution, friends of the cause of open access, profits from the sale of add-ons to the basic texts, funds freed up by the demise or cancellation of journals charging traditional subscription or access fees, or even contributions from the researchers themselves. There is no need to favor one of these solutions over the others for all disciplines or nations, and no need to stop looking for other, creative alternatives.



Book review: *We never expected that – a corporative study of failures in national and business intelligence* by Avner Barnea

Klaus Solberg Søylen^a

^a*Department of Engineering, Natural Sciences and Economics, Faculty of Marketing, Halmstad University, Halmstad, Sweden*

*Corresponding author: klasol@hh.se

Received 20 December 2021 Accepted 25 December 2021

We never expected that – a corporative study of failures in national and business intelligence. By Avner Barnea. (Lexington books, Lanham, Maryland, 2021)

For JISIB Barnea has previously written about competitive intelligence in Israel (2016), about Israeli start-ups in cyber security (2018), and about how AI will change intelligence and decision-making (2020).

The book, *We never expected that – A corporative study of failures in national and business intelligence*, is not on Israeli intelligence per se. Still, the best documented of the four cases presented come from the First Intifada in 1993 when Barnea was well situated to observe what was going on behind the scenes. For 27 years, until 1997, he was the Senior Official for Intelligence in the Prime Minister's office. Since then, he has been a competitive intelligence consultant, a teacher and student of intelligence studies and since 2016 a research fellow at the National Security Studies Center, NSSC.

The book, which is a translation of a book in Hebrew, which again builds on the author's PhD thesis, proposes an analysis of a series of intelligence failures. To study failures is a good way to learn. It is a good methodology, maybe the best. To present a book with both government and state failures is also a good idea from the perspective that there are bound to be fruitful parallels. So far so good.

Unless one speaks Hebrew, it's difficult to access experience gathered from within Israeli intelligence as so little is translated. Israeli

intelligence relies very much on an oral tradition of knowledge transfer which makes this task even more difficult. When we learn about how Israeli intelligence works and how the people working there think, the sources are often external, like in the classic book *Dangerous Liaison* by Cockburn and Cockburn (1991).

The aim of the book is to classify events according to the type of risk they represent. This is highly laudable and much needed.

The book starts with a claim: that intelligence methodology has reached a "glass ceiling," meaning an unacknowledged barrier to advancement in the intelligence profession. This could be true as it corresponds to findings in the intelligence literature. Barnea also argues that there have been too few parallels drawn between state and private experience of intelligence failures, which is also a fair claim. A weakness in the book is that it only builds on four cases, two from the private and two from the public sector. The empirical basis may, in other words, be limited.

The outcome of the exercise of the book is the presentation of a new dichotomy, or model, dividing "risks," or better "surprises," into "concentrated" and "diffused". The author claims that this will make a breakthrough in the intelligence field and the reader immediately wonders whether this claim can

be supported by the data presented. The notion of a “concentrated attack” refers to Handel (2003) in the book, but it’s actually from an earlier article by Handel published in 1984, described as a “deliberate and concentrated attack”. These attacks are planned by one actor carrying out plans (Singer 1958), through concealment and disinformation. The other type of attack is a “diffused attack,” defined as “surprise attacks, spontaneous and unplanned”. So, they cannot be predicted. So, we have one group of attacks that is planned and one that is unplanned.

It’s a weakness that there are not clearer definitions and that the dichotomy presented in the book is not discussed in greater detail compared to other existing theories that divide and try to understand the notion of risk. This goes back at least to what is called Knightian uncertainty, a lack of any quantifiable knowledge about some possible occurrence, as opposed to the presence of quantifiable risk. Knight’s risk is something that can be measured. That which cannot be measured is called “uncertainty”. So, following the Knightian notion of risk, there would be no case of a diffused risk that cannot be measured.

Barnea’s “diffused risk” may remind some of the notion, popularized by Rumsfeld, about “unknown unknowns,” or events we simply cannot know because even the idea of the type of risk is unknown to us. The idea is actually not Rumsfeld’s but goes back to the psychologist Joseph Luft (1916–2014). In 1955 he created a useful tool for illustrating and improving self-awareness, and mutual understanding between individuals within a group with his colleague Harry Ingham. They called the model the Johari Window model and it is shown in Figure 1.

Barnea’s unknown unknowns are of a special type: namely spontaneous and

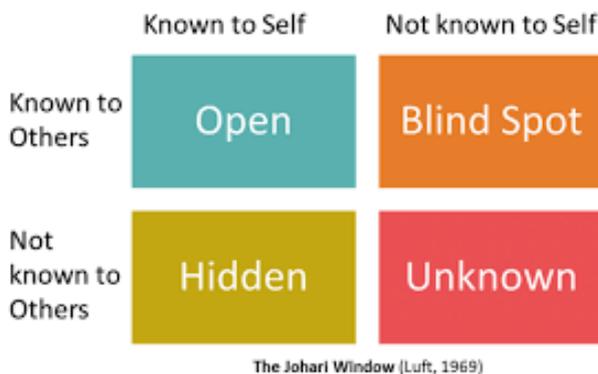


Figure 1 The Johari Window Model.

unplanned. We can also imagine non-spontaneous unknown unknowns and planned unknown unknowns. Unknown unknowns simply mean that others know, but we do not. They are events that are not even on our radar. In many cases they often speak more to our perception of the world and what may happen, and to our cognitive abilities.

Barnea’s concentrated attack could be said to be a known unknown, a “deliberate and concentrated attack” planned by one actor through concealment and disinformation. It is what we can know if we had a more capable intelligence organization.

The author uses the First Intifada and the 2008 recession as examples of diffused attacks, meaning they are surprise attacks, spontaneous and unplanned. One could argue that the first Intifada in December 1987 must have had a minimum of planning to be carried through, but the author does a good job at showing the complexity and uncertainty that led to this event, for example that riots broke out instantly without much PLO direction. There was a string of events which led up to it, including the killing of a Jewish person in Gaza followed by the killing of Palestinian workers in a civilian car. But there must have been a minimum of planning among those who came to the street. Anyway, the question becomes one of the degrees of planning.

The second example given by the author is the 2008 recession. This example is less clear. The recession was not deliberately planned of course, but it could have been foreseen as a result of reckless economic policies carried out in the US over decades. Many analysts did foresee it and have received much acclaim as analysts for having done so. Thus, it’s more difficult to see this example as a clear case of a “spontaneous” event. There were also many “surprises” in the recession, not the least the timing of the crisis, as is often the case with stock markets. It’s practically impossible to say exactly when they will unfold. You know something is brewing but it’s difficult to know at what date it will be disrupted. We are very much in a similar situation with the stock markets today, they could fall drastically in 2022. It’s more difficult to say in which quarter this may happen.

As examples of concentrated attacks, the author uses the 9/11 attack and the collapse of IBM in 1993. 9/11 was not planned by one actor, but it certainly was a “deliberate and concentrated attack”, and it was concealed. It was planned by an organization, al-Qaeda, not

by an individual, even though Khalid Sheikh Mohammed is often cited as the mastermind. Thus, the example is not difficult to accept, but the definition given by the author at the beginning raises questions as to whether the example was well chosen.

The last example presented by the author is IBM. IBM did not collapse in 1993 as it says in the introduction (“1993 collapse of IBM”), but in Chapter 7 this is adjusted to the headline “almost collapse”, which is more correct. In the late 1980s and early 1990s, the company faced difficulty after decades of success. However, the difficulties of IBM were not caused by one person or cause, but a series of incidents. It’s not clear to what degree this was an intelligence failure. One reason is suggested as: “This was because IBM’s core mainframe business had been disrupted by the advent of the personal computer and the client server. IBM couldn’t compete with smaller nimbler less diversified competitors.” Denning (2011).

CEO Thomas J. Watson Jr. suffered a heart attack and retired in 1971. After that the company had no less than four unsuccessful successors, until Louis “Lou” Gerstner took over in 1993. Gerstner, CEO of IBM from 1993 until 2002, turned the company around mainly by starting to listen to its clients, according to Denning (2011). The intelligence effort this implied, for example starting an official competitive intelligence function and office at IBM, has been noted by many authors, for example Behnke and Slayton (1998) and Prescott and Williams (2003).

At the end of the book the author suggests how methods/activities can be transferred from business intelligence to national intelligence and vice versa. The book consequently uses the term “business intelligence” (BI) as was common some decades ago before BI became all about software and not about “competitive intelligence” or “market intelligence” when appropriate. This can be confusing to some readers.

The author notes that for BI it’s about sharing information internally, relying more on open source and measuring the value of information. For national intelligence to BI it’s about defining key intelligence topics and using competing hypotheses (“analysis of Competing Hypothesis, ACH), as developed by Richards (Dick) J. Heuer, Jr., of the CIA in the 1970s, building on abductive reasoning. These are probably good conclusions, but I expect that they come from a much larger amount of experience, which the author has not shown

through the four cases presented in the book. The book is valuable more because of the collective experience that Barnea brings into the conclusion in Chapter 8 than because of what can be drawn out of the model, or the cases used. What makes Barnea’s book especially interesting is how the author brings experience from the state sector to the private sector and vice versa, having worked in both sectors himself.

REFERENCES

- Barnea, A. (2015). Failures in National and Business Intelligence: a Comparative Study. *PhD Diss., University of Haifa*, 66-129.
- Barnea, A. (2016). Study on competitive intelligence in Israel: 2016 update. *Journal of Intelligence Studies in Business*, 6(2).
- Barnea, A. (2018). Israeli start-ups—especially in cyber security: Can a new model enhance their survival rate? *Journal of Intelligence Studies in Business*, 8(1).
- Barnea, A. (2020). How will AI change intelligence and decision-making? *Journal of Intelligence Studies in Business*, 1(1).
- Barnea, A. (2021). *We Never Expected That: A Comparative Study of Failures in National and Business Intelligence*. Rowman & Littlefield.
- Behnke, L., & Slayton, P. (1998). Shaping a corporate competitive intelligence function at IBM. *Competitive Intelligence Review: Published in Cooperation with the Society of Competitive Intelligence Professionals*, 9(2), 4-9.
- Cockburn, A., & Cockburn, L. (1991). *Dangerous liaison: the inside story of the US-Israeli covert relationship*. HarperCollins.
- Denning, Steve (2011). “Why did IBM Survive”, *Forbes*, Jul 10th
- Handel, M. I. (1984). Intelligence and the problem of strategic surprise. *The Journal of Strategic Studies*, 7(3), 229-281.
- Kahana, E. (2006). *Historical dictionary of Israeli intelligence*. Scarecrow Press.
- Knight, F. H. (1921). *Risk, uncertainty and profit* (Vol. 31). Houghton Mifflin.
- Prescott, J. E., & Williams, R. (2003). The user-driven competitive intelligence model: a new paradigm for CI. *Competitive intelligence magazine*, 6(5), 10-14.

Singer, J. D. (1958). Threat-perception and the armament-tension dilemma. *Journal of Conflict Resolution*, 2(1), 90-105.