Information Security and Public Diplomacy: Lessons from the Past, a Look at the Future

Hirsh Goodman

"The way in which the State of Israel handles its most secret and sensitive information is incomprehensible and in many ways irresponsible. Considerable damage has already resulted and more will be caused unless there is a change in this regard. Without immediate, determined, and stringent action taken at both the government and military levels, the consequences could be disastrous." [1]

The Information Security Challenge

The problem of information security – or field security, to use the traditional term – is as old as war itself. The need to protect information about one's strengths, vulnerabilities, and intentions is elementary, and some would argue as critical as intelligence gathering.

The Winograd Commission devoted fifty pages, some twelve per cent of its findings on the Second Lebanon War to the issue of information security, and states categorically that in this essential area there was a serious failure that endangered human lives and impeded the IDF's room to maneuver.[2] It cites the head of the Information Security division acknowledging at a meeting in the office of the chief of staff on November 26, 2006 that the exposure of Israeli forces was "extremely high" during the war, with the result that the IDF's freedom in conducting the war was compromised and Israel's intelligence advantage placed in jeopardy.[3]

There were many factors that contributed to this lapse, including that the IDF itself did not take into account the implications for information security in the event of an all-out war with Hizbollah and failed to organize to meet the challenge. In addition, the chief of staff and the IDF Spokesman's Unit opted for a policy of openness[4] with the media during the war, though without consulting the head of Information Security or taking into account the operational consequences of not consulting him. Thus, senior military officers went to talk to the press without being briefed in advance on what and, more importantly, what not to say; their reports were broadcast worldwide in real time, effectively bypassing the censor. This was also true of the legions of former senior military officers, many of them with close ties to the military and decision makers conducting the war, who appeared live on Israeli and foreign television with their analyses of the war and its (mis)

Hirsh Goodman, senior research associate at INSS

management.[5] Add to this the informed leaks from the Cabinet and inner Cabinet that, according to the report, were published in real time and caused serious harm to both public and military morale, as well as imparting important information to the enemy.[6]

The report is an insightful window into the complexities faced by those charged with information security in the age of modern warfare. The report is meticulous in its handling of issues such as the public's right to know versus censorship and security, the role of the media, and freedom of speech in a democracy, but its bottom line is that because information security failed, Hizbollah acquired critical intelligence assets during the war, mainly from live broadcasts from Israel that disclosed in real time where rockets were landing, what strategic targets were narrowly missed, and how Israel's emergency services were responding. It was also possible to gauge how public morale was faring and what political disputes were nurtured as a result of the war. Hizbollah's most trusted sources of information were seemingly Israel's three news channels, whose correspondents Hizbollah correctly considered extremely well informed.[7] No wonder, then, that former chief of staff Dan Halutz assessed that the intelligence Hizbollah gained from the Israeli media during the war was worth "hundreds of millions of dollars."[8] The Winograd Commission called it priceless and judged that it seriously impacted on the IDF Command's ability to conduct the war freely.

Within the military it is easier to introduce information security awareness and impose discipline than within the political sector. Communication systems are integrated and centralized, allowing for tight control, and there is a hierarchy of command that can oversee the implementation of information security policy. Indeed, the IDF has already acted on some of the failings cited in the report. All army cell phones, other communications equipment, and beepers are now coded. Officers are under very strict orders not to speak to the press without authorization. Cell phone use in units has been severely restricted. There is tighter coordination between the IDF Spokesman's Unit, the Information Security Unit, and the censor. The chief of staff and head of Military Intelligence have both taken a more proactive role in this regard.

The danger of leaks has likewise been emphasized on the civilian level, and the Cabinet secretary has taken steps to tackle the phenomenon.[9] Similarly, despite Israel's propensity for leaks, the Winograd Commission is adamant on not capitulating to this norm among the political echelons. Much can be achieved by limiting forums to those who need to know, tighter control on staff, threat of penalties, and closer policing by the General Security Services, which is charged with guarding the country's secrets.

Nonetheless, the main problems remain: the ever-growing intrusiveness of the press; technologies that allow audio and video transmission from anywhere to everywhere in real time; the insatiable appetites of 24-hour, 365-day-a-year news stations, and the limitless possibilities of information dissemination on the internet. And because the next battlefield will in all probability again be the home front where it is not always possible to close off areas to the media, it can be expected that the intrusive eye of the media will be everywhere, all the time.

Moreover, in the age of modern transmission technologies it can be assumed that once out, information cannot be contained. The

job of those in charge of information security is to prevent sensitive information from reaching the public domain. The censor's job is to prevent its dissemination. The censor, however, is the last bulwark and only works when those disseminating the information volunteer to submit it for perusal. There are laws that demand that journalists bring certain issues – such as contacts with countries that Israel does not have relations with, oil purchases, immigration, and information pertaining directly to Israel's security – before the censor and face legal action if they don't, but submission remains voluntary and cases of prosecution are rare. And even with massive resources, there is no way the censor can police all the channels of transmission in this day and age when a modest cell phone can broadcast audio and video images and the internet is freely accessed. Information security cannot begin with the censor nor can the censor be relied on to stop security breaches. Once sensitive information is in the public domain one has to assume it will be disseminated. The concerted effort in terms of information security, therefore, has to be in preventing initial disclosure, since stopping the messenger is essentially a futile task.

The Role of Public Diplomacy

Information security does not stand by itself nor is it the sole responsibility of the security branches charged with implementing it. Complementing it are the country's public diplomacy policies, particularly surrounding events that attract extensive media attention.

In the Second Lebanon War the army spokesman's office decided on a policy of openness with the media, whose principles were laid out by the chief of staff in an address to senior officers in June 2005, a year before the war. Then-Chief of Staff Halutz said the presence of the media is a reality that has to be taken into account, and called for an "open and controlled" relationship which the army spokesman then translated into policy.[10] Indeed, during the Gaza disengagement two months later the IDF maintained a successful policy of openness with the media, with camera crews and reporters attached to units and accurate reports emerging from the field.[11] The American experience of embedding reporters with troops in the 2003 Iraq War also had positive results. Conversely, when Israel refused reporters access to its operations like the 2002 incursion into Jenin,

the world was falsely led to believe that Israel had committed a massacre there.[12]

What worked in Gaza, however, did not work one year later, and for many reasons. The Gaza pullout was a civilian operation – albeit performed by soldiers – that did not involve an enemy or occur during a state of war. The area in question was geographically isolated and thus easy to control, and partly in an effort to package the event for the media, troops were trained on how to deal with the resident population.

In the Second Lebanon War, however, the entire northern sector of the country was a battlefield offering almost unfettered access to journalists broadcasting vital information to the enemy in real time. Recruitment and rallying points were open to the eye of the media, which could see and broadcast what weapons were going where and what casualties were incurred. There was no advance media training, the sources of information were not controlled, and reservists with colleagues and friends in the media and senior officers with their own agenda were shaping the mood of the day. As part of the policy of openness it was decided that the army would provide the media with multiple spokesmen and provide as many briefings as possible. The theory was that to control the message one has to ensure that there is no vacuum in media coverage that could be used by others to your disadvantage. Yet the result was a flood of uncontrolled and damaging information reaching the public, which was deemed by the Winograd Commission to have resulted in serious consequences for Israel and serious gains for Hizbollah.

An attempt to find a mechanism to manage an effective public diplomacy policy has come to life in the form of the National Intelligence Directorate.

What emerges, therefore, is that a public diplomacy policy, though successful in one context, cannot arbitrarily be grafted onto another. In order not to repeat the mistakes of the last war in terms of providing the enemy with real time information on the accuracy of its attacks, the security services would do well to develop the ability to close off certain zones to the public in times of emergency. Given Hizbollah's trust in the information gained from Israeli news broadcasts, it is important to consider how the information can work to Israel's advantage. Since there is a high probability that the next war will involve civilians, the Home Front Command should be factored into the media cycle and supplied with competent spokespeople. This will necessitate a wide network and meticulous training including on issues of information security. A policy of openness is inevitable given the ubiquitous nature of the media, but as the former chief of staff stipulated, it has to be controlled and messages have to be clear, credible, unified, and gleaned of all sensitive information in coordination with the relevant authorities.

An attempt to find a mechanism to manage an effective public diplomacy policy has come to life in the form of the National Intelligence Directorate, a unit in the prime minister's office that became functional in early 2008 and coordinates Israel's public diplomacy efforts, including those of the Foreign Ministry, the Prime Minister's Office, and the IDF Spokesman's Unit. In the past there have been severed ties between these three branches with bad results: mixed messages, confusion, non-credible information, and the antagonism between the state and the local and international media. The new body has yet to be tested in times of national emergency but its positive imprint has already been demonstrated.

For example, on April 29, 2008 an Israeli missile fired from a helicopter resulted in the deaths of a mother and four children in the Dir el-Balagh refugee camp in the northern Gaza Strip. Despite the severity of the story and its potentially negative consequences for Israel, quick action by the Directorate managed to limit the damage and instill doubt that the family was killed by an Israeli missile. It quickly issued a credible explanation, later backed up with hard evidence, that the family was actually killed when two armed men carrying explosives en route to an attack on Israel were intercepted from the air: the explosives they were carrying, and not the Is-

raeli missile, destroyed the house and killed the family. Subsequently, prominent news outlets like T*he New York Times* carried both the report that the family had been killed and Israel's version of how it happened.[13] Getting Israel's version out to the media in almost real time indicates a new level of cooperation between the IDF, which supplied the information, the new Directorate and elsewhere in the Prime Minister's Office, which crafted the message, and the Foreign Ministry, which disseminated it.

Conclusion

The need for synergy between the IDF Spokesman's Unit and the unit charged with information security and the censor is one of the key findings of the Winograd Commission and critical to the implementation of a sensible policy that recognizes the reality of the media but limits the exposure of the country's secrets. In the case of disclosure of information it is not possible to kill the messenger, and once information gets out it will become public. Therefore, it is imperative to inculcate those trusted with the country's secrets to guard them. Leaks have to be plugged and information to be made public has to be filtered in advance by the relevant authorities. A policy of openness with the media is both essential and desirable, but the process must be controlled and tailored to specific situations. That is the main thrust of the Winograd report's recommendations and those responsible for the country's security would do well to take it into account.

Notes

1 Winograd report, p. 473, article 211.
2 Winograd report, p. 456, article 121; p. 473, article 210.
3 Winograd report, p. 457, article 122.
4 Winograd report, p. 452, articles 104-7.
5 Winograd report, p. 456, article 119.
6 Winograd report, p. 468, articles 186-89.
7 This subject is dealt with in depth by both the Winograd report and the chief of staff in an interview with *Yediot Ahronot*, February 15, 2008.
8 Interview with *Yediot Ahronot*, February 15, 2008.
9 Interview by the author with IDF Spokesman, March 2008.
10 Winograd report. p. 452, article 106.
11 See *Seventh Eye*, Vol. 64, Sept. 2006.
12 Hirsh Goodman and Jonathan Cummings, eds, *The Battle of Jenin: A Case Study in Israel's Communications Strategy*, Memorandum no. 63, Jaffee Center for Strategic Studies, 2003.
13 Ethan Broner, *New York Times*, April 29, 2008.