BESA
The Begin-Sadat Center for Strategic Studies
Bar-Ilan University
PERSPECTIVES
THE BEGIN-SADAT CENTER FOR STRATEGIC STUDIES

The "Unclassified Secret"

by Dr. Natanel Flamer and Lieut. Col. (ret.) Erez Magen

BESA Center Perspectives Paper No. 2,238, November 26, 2023

EXECUTIVE SUMMARY: The Hamas attack on October 7 was formulated based on intelligence gathered by the terrorist group in advance, a significant proportion of which was unclassified civic or non-strictly classified military information. This reflects a broader phenomenon defined as "unclassified secrets" - information which, while not classified, nevertheless holds considerable or even critical value to an adversary. To establish guidelines to deal with this phenomenon, its complexity has to be acknowledged. Due to the open availability of such information, any means of controlling it will require a nuanced approach that balances democratic concerns about freedom of information and the public's right to know with security needs.

Hamas gathered information on Israel, much of it unclassified, and successfully used it to carry out the largest and most devastating terrorist attack in Israel's history.

At the core of every advanced organization's information security and cyber defense lies a mechanism for risk management. This mechanism weighs the likelihood of the realization of intelligence and technological threats against the potential damage resulting from an information leak. Risk management allows a focus on the protection of significant assets and ensures, as much as possible, that threats against them will not succeed. The less favorable alternative is "protecting everything," an approach guaranteed to be ineffective due to endless "secrets" and limited resources.

This article seeks to describe a phenomenon we call the "unclassified secret," meaning information that is not classified by definition but which still holds great value for an adversary seeking to harm a country or organization. In a democratic and open society, the freedom of information is fundamental. The ability of people in society to share information is vital for progress and development. It provides the infrastructure for citizens to be engaged, oversee the authorities, criticize them, and form independent opinions through free and reasoned discussion. In this way, civil information, or unclassified security information, is accessible to everyone – including foreign actors and enemies – especially as platforms for its distribution and accessibility continue to evolve.

The events of October 7 will be investigated and examined with great care, but it can already be said that Hamas constructed a good intelligence puzzle of Israel's defense components along the border fence. This enabled Hamas to neutralize some of the sensors and detection capabilities, prevent effective control of events on the Israeli side, and operate effectively within the bases, outposts, and settlements they invaded. In addition to military information, Hamas had civilian, private, and administrative information that facilitated its operations within the attacked communities. Apart from maps available to everyone, it is evident that Hamas had information about specific sites within the settlements, some of which can be found online (such as addresses of senior officials) and information that could be collected through human sources (HUMINT), such as the locations of first response teams, concentrations of soldiers and civilians, defense perimeters of the settlements, and more.

Examining the security information collected by Hamas over the years reveals that a significant part of its intelligence is based on information that is not classified by definition. For example, most of the human collection elements (HUMINT) recruited by Hamas were instructed to mark locations throughout Israel that are visible to all. In addition, Hamas collected a wealth of information from Israeli media about Israeli society, issues related to the settlements surrounding the Gaza Strip, and Israel’s military capabilities, all of which was discussed openly.

These facts together constitute a particularly challenging phenomenon that we refer to as the "unclassified secret." This is information that is either civilian or defined as unclassified by the authorities, yet highly valuable to hostile actors that

collect it for their purposes. In the case of a terrorist organization like Hamas and an attack like the one it carried out, tactical and micro-tactical information defined as unclassified, as well as civilian information that is openly accessible, become extremely valuable, especially when it provides details that complement information collected from other undisclosed intelligence sources operated by Hamas or any other organization. Thus, in the case of a terrorist organization, civilian information that is sometimes considered insignificant takes on a critical value. The unclassified space contains "secrets" that must be treated appropriately.

At this point, one might argue: If such information is valuable for the enemy, why isn't it classified? The deeper question that then arises is this: How far can the concept of "classified information" be stretched? Information classification expresses the potential risk and damage that would result from exposure to an unauthorized party. Consequently, the basic definition of classified information is information that, if exposed to an unauthorized party, could harm the security of the state or other "owner of the secret." But harm to the security of the state in what sense? For example, in a scenario in which terrorists plan to attack settlements on the Gaza border, maps of Israel that are available on Google Earth constitute valuable information for the enemy. Surely one cannot have the internet scoured of all such information due to its potential use by terrorists.

The other extreme is to say the unclassified secret is the inevitable bane of a democratic and open society, especially in areas of risk and near hostile borders, and there is nothing that can be done to reduce the risk inherent in the phenomenon.

Faced with these two extremes, neither of which seems to contain the whole truth, we should delineate a few guiding principles with which to approach situations in which unclassified secrets of a kind highly valuable to the enemy are widespread.

Unclassified information must be addressed systematically in the context of the impact of civilian knowledge of security components that enable the enemy to exploit it for operational purposes. The "unclassified" space must be addressed within situational assessments while realizing and considering its value to the enemy.

In this context, attention should be given to civilian "information baskets" that require investment in protection, monitoring, and control, including:

- Civil security components: first response teams, civil-military relations, settlement defense systems, and reinforcement forces.
- Human concentrations that could serve as prime targets for attack, both permanent and occasional (public transportation stations, event halls, parks, etc.).
- Residences of senior officials, security personnel, local leaders, etc.
- Technological assets (websites, servers, cameras, etc.) in the civilian space.

Within this framework, the trend should be towards reducing the ease of obtaining non-essential civilian information, such as: protecting databases according to privacy protection regulations, defining target groups who are prohibited from keeping a high personal digital footprint, monitoring digital misbehavior and issuing warnings for prevention and damage reduction, and even considering tighter censorship. Regarding military information that is published for various reasons by security officials, the balance between their needs and information security must be reevaluated. As in many cases, this information becomes "unclassified secrets": information approved for publication by the authorities that ends up aiding the enemy.

For example, in the context of the human threat, when Hamas openly trains and declares its intention to attack communities on the Gaza border, this should prompt a reconsideration of permit policies so as to prevent the possibility of Gazan workers, or those with potential connections to the powers in the Gaza Strip, working in these communities and gaining access to unclassified secrets. Similarly, increased awareness is needed regarding intelligence-gathering by civilians around security sites and sites of human concentration.

The interface between the security and civilian spaces, and between the unclassified and classified spaces, poses a significant challenge when trying to provide a fitting and balanced response to the problem of unclassified secrets. The formation of security policies in this context is complex and will require attention, resource allocation, legislation, and broad cooperation. The need to maintain maximum information freedom while recognizing security constraints - a

challenge that accompanies democracies worldwide, including Israel - will only continue to grow.

Of course, even after the formulation and implementation of policy guidelines, the reasonable working assumption is that the enemy will continue to obtain valuable information. Accordingly, in all defensive arrangements, military or civilian, practical consideration should be given to the information load that the other side has, including unclassified yet useful material. Correspondingly, a complementary defensive or offensive response is required.

The battle over unclassified secrets is here to stay. We must be aware of it and prepare ourselves accordingly.

Dr. Natanel Flamer is a senior lecturer in the Department of Middle Eastern Studies at Bar-Ilan University and senior researcher at the Begin-Sadat Center for Strategic Studies. He is the author of "Hamas Intelligence Warfare Against Israel", forthcoming from Cambridge University Press. Dr. Flamer specializes in intelligence, terrorism, and asymmetrical warfare in the Middle East.

Lieut. Col. (ret.) Erez Magen is Information security and cybersecurity expert, founder of Magen Cyber, which provides security solutions to security organizations and companies in Israel and around the world.