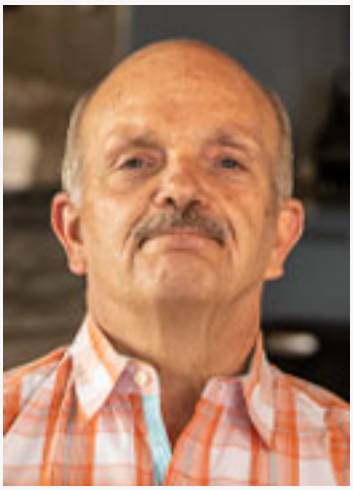
Steve Cocco, FBI Veteran and President Of Security Strategies Today, Talks About "The Intelligence Cycle"...

...following the horrific terrorist attacks perpetrated by Hamas against innocent civilians in Israel, "In The Boardroom™" On www.SecuritySolutionsWatch.com



Steve Cocco, President, Security Strategies Today

Private Investigations | Business Continuity and Crisis Management
Security and Threat Vulnerability | Use of Force Consulting

www.SecurityStrategiesToday.com

PHOENIX, ARIZONA, USA, January 10, 2024 /EINPresswire.com/ -- On October 7, 2023, the world witnessed brutal and horrific terrorist attacks perpetrated by Hamas against innocent civilians in Israel. The attacks are said to have caused the death of at least 1,200 Israelis and citizens of other nations and some 200 hostages were taken. In response, Israel has vowed to eliminate the terrorist organization and has pursued a path of nearly uninterrupted military strikes against Gaza, including what it claims to be terrorist operational and support structures hidden among civilian infrastructure.

> We are honored to speak with Steve Cocco today about "The Intelligence Cycle" following the horrific terrorist attacks perpetrated by Hamas against innocent civilians in Israel."
>
> *Martin Eli, Publisher*

Initially, in what has been characterized as one of the most shocking intelligence failures since the Al Qaeda attacks against the United States on September 11, 2001, the Israeli government, despite its vast and far-flung intelligence gathering apparatus, did not detect the detailed and precise planning that such abroad-based attacks required. Because of this abject and complete failure, it took no measures to prevent them or to "neutralize" the attacks before they were carried out.

A shocking new report from the New York Times indicates however that, according to the sources it consulted in drafting the article, the Israeli government

had in fact received at least some reporting that Hamas was planning a large, multi-pronged siege that would strike Israel using various means and at several locations, disseminating death and carnage and causing long-term anxiety and fear at a level not seen since the creation of the state of Israel in 1948. If the reporting is accurate, the sheer negligence and incompetence of government officials at their failure to act can be added to the complex mix.

Why is it a complex mix? Consider that an effective intelligence "cycle" is a foundational element that any responsible government acting in the interests of its citizens must make use of. Everything from protecting troops and military bases at home and abroad, to deploying effective countermeasures to thwart cyber attacks and defend critical infrastructure, depends on timely and accurate intelligence. If a government is not constantly updating, assessing and reevaluating its intelligence needs and adjusting intelligence priorities, then it risks falling victim to myriad attacks emanating from any number of perpetrators.

The intelligence cycle is a "living" or dynamic process. It is complicated in that it impacts many divisions or branches of a government. But it necessarily involves rigour and strict methodology.

Let's take a closer look at some key aspects of intelligence gathering and comment on how they impact decision making:

1. Determine Intelligence Needs:

A government needs to be candid and recognize that what it does not know can in fact be detrimental to its citizens. For example, if a nation is experiencing a significant influx of illegal migrants, as is the case in both the United States and in the European Union, then an intelligence gap might be having an incomplete or fragmentary understanding of the criminal enterprises behind the organized trafficking of migrants. The need then exists to fill that gap. Without such knowledge, combatting migrant trafficking effectively would be nearly impossible.

Another intelligence gap could be identified during the process of implementing a wide-ranging, new government regulation or law. Readers may recall the widespread violence and destruction of property that took place in many French cities after the government pushed through its pension reform earlier in 2023-a measure that raised the retirement age of French workers to 62. The backlash among the public overflowed onto the streets, causing destruction of property, including looting and violence. The government certainly might have anticipated some protests-but the intensity and virulent nature seemed to take officials by surprise. Most likely, the French government either ignored intelligence about the organizing of protests, did not have adequate

sources deployed to start with and/or did not analyze thoroughly the intelligence that it did collect. Somewhere, someone dropped the ball.

These intelligence gaps or needs must be addressed so that policymakers can anticipate the actions of others and neutralize or contain them, if deemed appropriate. The gaps can only be filled if appropriate sources are brought to bear. One cannot wait for intelligence just to "arrive" via a newspaper report or media speculation. At that point, it's often too late to thwart an attack or other acts of violence or civil unrest. Only a multi-pronged approach to intelligence gathering is likely to result in useable or actionable intelligence that can detect and neutralize attacks, prevent organized disruptions to services (such as denial of service, or "DOS" attacks) or anticipate the actions of bad actors.

Addressing these needs through the gathering and assessment of actionable intelligence is accomplished, in part, through the deployment and management of sources.

2. Identify and Deploy Sources:

Once intelligence needs have been identified, then the deployment of sources to gather useful, timely and actionable intelligence is the next step. These intelligence sources can be human or can be technical in nature.

Going back to our discussion of the October 7 attacks in Israel, it seems likely that the Israeli government did not have even the most basic insight into what the Hamas leadership was planning. Or, if it did have an idea that the attacks in fact were being planned but failed to act, then the intelligence process followed was even more seriously flawed. That is to say, if Israeli officials deemed that the Hamas plan was simply "aspirational", as the article alleges and/or that the group was incapable of carrying it out, what led them to believe this? What was this assumption based on? Had they not kept up to date on the group's training, access to weapons, objectives, manpower, etc?

Assumptions reflect our beliefs that certain events or situations will or will not take place, evolve or remain constant. But there is always a degree of uncertainty in assumptions-they would be called certainties otherwise!

Whatever the assumptions were regarding Hamas, they were incorrect. Now it is incumbent upon Israeli officials to determine where they went wrong. In their investigation, which must be all-encompassing regarding the intelligence capabilities of its own government agencies, they must start from scratch and ask some key questions, among them:

Did agencies redirect resources to other targets they deemed more worthy, thereby creating a greater deficit in their knowledge and understanding of Hamas? An example would be if they changed their focus and prioritized collection on threats to the northern border with Lebanon, or on threats emanating from the occupied West Bank. What lead them to do this, if it in fact

occurred?

If several hundred men and possibly women participated in the planning and execution of the attacks, how did Israel fail to detect such extensive targeting and planning? These attacks were complex in their coordination and execution.

Finally, in answering the above questions, Israeli officials need to consider that at least some of those human sources they believed to be loyal to them were in fact working for the other side. In other words, the Israeli confidential sources were "doubled" against them and they were actually feeding their handlers false or misleading information. Not uncommon with sources, but if that is the case then one must question how thoroughly these sources were evaluated and if such evaluation was conducted regularly.

The technical sources of information that Israel relied on in part in assessing Hamas also need to be reevaluated. As the attack went undetected or was dismissed as aspirational, then these technical capabilities were directed at targets which did not have access to current leadership or decisionmakers. They might have been properly targeted at inception, but they went silent or were compromised by Hamas at some point in time.

3. Assessing and Evaluating Source Information:

This is a key component that requires a holistic approach. In other words, if a source of information is reporting on a group's plans to, for example, smuggle tons of drugs and precursor chemicals into the United States, what other sources are saying the same or similar things? In other words, with few exceptions, intelligence derived must be corroborated. Divided or conflicting loyalties of sources is something that must always be considered as a factor influencing source reporting. Therefore, corroboration by independent sources is essential.

These are but a few of the many factors that should have been followed strictly and routinely by Israeli officials in what should be frequent assessment of its intelligence needs with regard to Hamas. The same dynamic and continuous process is required when evaluating other threats that may impact the nation, from human trafficking to organized crime infiltration of business and of course, the threat stemming from other terrorist formations, such as Hizballah.

This article is geared at providing general but hopefully insightful information on some common elements that come to mind when talking about intelligence and its use in decision making. For more information about what we do, check out our website at
www.securitystrategiestoday.com
****

For the complete interview with Steve Cocco, please click here:
https://www.securitysolutionswatch.com/Interviews/in_Boardroom_SecurityStrategies_Steve_Co

cco.html

Connect with Steve Cocco on LinkedIn: https://www.linkedin.com/in/stevecocco/

****
****

About SecuritySolutionsWatch.com:

_____

www.SecuritySolutionsWatch.com features thought leadership and content-marketing regarding: AI, Biometrics, Cybersecurity, FinTech, IT, IoT, Robotics, Physical Security and “back-to-work” solutions. Our flagship “IN THE BOARDROOM™” platform, since 1999, has featured brand awareness and lead generation programs for leading global brands such as: Allied Universal, ASSA ABLOY, AT&T, Cisco, Dell EMC, Fujitsu, GE, Gemalto, Honeywell, HPE, IBM, Intel, McAfee, Microsoft, Panasonic, SAP, Siemens, Stanley Security, Symantec, UNISYS, and many SME’s, in the USA, EMEA, and APAC.

What’s YOUR Solution?

Want to be featured “In The Boardroom™” and benefit from this type of media coverage? Please contact us here for more information:
https://www.securitysolutionswatch.com/Main/Contact_Us.html

****
****

Martin Eli, Publisher
SecuritySolutionsWatch.com
Editor@SecuritySolutionsWatch.com
Visit us on social media:
Twitter
LinkedIn
