POSSIBILITIES AND CHALLENGES OF PREDICTIVE PROFILING IN THE STATE BORDER GUARD

Juris Madžuls[1], Daina Znotiņa[2]

[1] Mg.soc.sc, docent, the State Border Guard College of the Republic of Latvia, e-mail: juris.madzuls@rs.gov.lv, Rezekne, Latvia

[2] Mg.soc.sc, lecturer, Rezekne Academy of Technologies, e-mail: Daina.Znotina@rta.lv, Rezekne, Latvia

Abstract. *The paper is aimed to investigate the role of predictive profiling (hereafter PP) in the fight against cross-border crime and terrorism. The main tasks of the article are to describe the content of PP, the added value of its implementation and how it can be used in the State Border Guard Service of the Republic of Latvia (hereafter SBGS) as a complement to risk assessment in operational situations. The authors of the paper explores the content of the PP implemented in the Royal Netherlands Marechaussee (hereafter KMar), as well as in Slovakia, Spain and several Central Asia region countries. For this purpose analysis and evaluation of documents, scientific, pedagogical and psychological literature was performed and suggestions for the improvement of border guard service threat detection system in the field of PP were compiled.*

The paper outlines the goal of PP, which is to identify, assess, and take action on a potential criminal or terrorist threat as early as possible (preferably during preparatory actions). Deviant behaviour in combination with Attacker Method of Operation forms a key concept. The AMO provides the indicators for the deviant behaviour. Furthermore, the paper delves into the system of PP and its corresponding process steps. PP is focused on the threat, not the risk, making it a threat analysis.

Keywords: *border guard, predictive, profiling, risk, threat.*

History of Predictive Profiling

The foundation for PP was laid by Colonel *John Boyd* of the US Air Force, who became America's most influential military theorist. He established the basis for thinking about profiling and had a significant influence on assessment and decision-making processes within the US military through his theories, particularly the OODA (Observe, Orient, Decide, Act) loop (also known as the "decision cycle"), which was developed to help pilots make quick decisions when engaging in air combat (Boyd, 1996).

American professor *Paul Ekman* originally focused on nonverbal behaviour and by the mid-1960's concentrated on the expression and physiology of emotion. He has also had a long-standing interest in interpersonal deception. To train police and other people's profiling skills Paul Ekman used simulators that were developed based on the FACS (face signals description).

In the late of 1970s, profiling was firstly applied by Israeli airline "El-Al" during ramp inspections in response to growing extremist terrorist

https://doi.org/10.17770/bsm.v5i10.8306

activities. It was a direct response to the attack on *Lod* airport (now *Ben Gurion* Airport) in Tel Aviv by the Japanese Red Army, recruited by a Palestinian extremist group, which resulted in many casualties on May 30th, 1972 (NPA, 2024).

The first successful implementation of PP took place during the "*Hindawi Affair*", where EL AL security personnel prevented an attack on an EL AL flight from London to Tel Aviv. The technique was later refined by Israeli Intelligence and Security Services.

After the September 11th, 2001 attacks, profiling techniques were further developed by mainly American intelligence agencies. Today, these techniques are applied worldwide by law enforcement authorities and became very interesting for commercial applications.

PP stands out because it focuses on identifying behaviour that deviates from the norm, specifically related to the modus operandi of criminals or terrorists. This is in contrast to the approach of Israeli services before the *Hindawi* incident (Staff, 2021), where ethnicity and gender were emphasized. This changed, particularly after the first and second *intifadas* (Palestinian uprisings), during which terrorist organizations started using women and children as suicide bombers. This modus operandi was also frequently employed by terrorist organizations like the *Tamil Tigers* in Sri Lanka (Britannica, 2024).

Boyd's OODA Loop

The cyclical, dynamic OODA process was originally introduced by United States Air Force Col. John Boyd as a strategic method for conceptualizing battlefield decision making. Boyd proposed that successful military decision making required fast, agile human decisions, not just larger machines or more deadly weaponry. His tactical theories derived from his studies of fighter pilot combat dogfights (both Korean and Vietnam Wars) and historical combat strategy dating back to Sun Tzu (Boyd, 1987). He argued that the goal of military tactics should be to operate in a manner to get inside of the adversary's decisions and actions, to "…enmesh the adversary in a world of uncertainty, doubt, mistrust, confusion, disorder, fear, panic, chaos, … and/ or fold adversary back inside himself so that he cannot cope with events/efforts as they unfold" (Boyd, 1987). The aim of this model is to make decisions and take action faster than the opponent, thereby neutralising and defeating them. This is achieved by anticipating the opponent's next move (essentially putting oneself in their shoes) and reacting faster than they can adapt.

Note importantly that the OODA loop is a conceptual or descriptive model, not a detailed process model. Indeed, it is often reported, or

criticized, for being one of the more high-level descriptions of time critical decision making (Azumaet al., 2006). The OODA loop might be thought of as a simple representation of a control process, where the internal operations of the human adjust to the external changes in the environment. However, though there is a tendency for some accounts of the OODA loop to draw a simple 4-stage loop, the OODA loop as originally conceived is not that simple (Blaha, 2018).

The OODA Loop is an extremely effective thinking and decision-making model presented in the form of a circular process and can be seen as a comprehensive system. The OODA Loop, considered an interaction model with the environment, consists of four sequential steps (Boyd, 2018):

- **O**bserve/Perceive: The first step is to identify the problem or threat and gain an overall understanding of the internal and external environment. In the military world – gathering data through observation. In the corporate world, this can be equated to collecting current information from many sources as quickly as possible and be prepared to make decisions based on it.
- **O**rient/Analyse: Analysing, interpreting and reflecting on what has been found during observations and considering what should be done next with purpose to update organisation current reality. The Orient phase requires a significant level of situational awareness and understanding to make a conscious decision. Since some decisions are unconscious or instinctual, this step involves considering what and why decisions are made prior to choosing a course of action. When applied on an individual level, the Orient step can be performed by creating mental models or mental rehearsal drills to place information into narratives that shape judgement. In organizational applications, situational models can be created with machine learning tools to identify potential outcomes, while removing any bias.
- **D**ecide: This phase makes suggestions toward an action or response plan, taking into consideration all potential outcomes. This can be accomplished through meetings or discussions that are focused on creating a roadmap for the entire organization.
- **A**ct: Action pertains to carrying out the decision and related changes that need to be made in response to the decision. This step might also include any testing that is required before officially carrying out an action, such as compatibility or A/B testing.

These phases have been broken out for the purposes of explanation, but in some real-world scenarios, they might happen in a fraction of a second. One key to the success of the OODA loop is to make it as short as possible, minimizing reaction times in high-stakes situations. The ability to

make decisions faster than an opponent is important, but it is not only about speed. Tempo – frequency – is also critical, as the ability to rapidly speed up and slow down can generate unpredictability. Being unpredictable makes it difficult for opponents to understand and adjust themselves to what happens next. Cycling through an OODA loop with more tempo than an opponent gives an organization more control of the environment and a better chance of succeeding.

Observing and orienting correctly are key to making a successful decision. If these steps are flawed, they'll lead individual to a flawed decision and subsequently a flawed action. So while speed is important, so is improving individual analytical skills and being able to see what's really happening.

The figure 1, demonstrates that the OODA loop operates as a system.

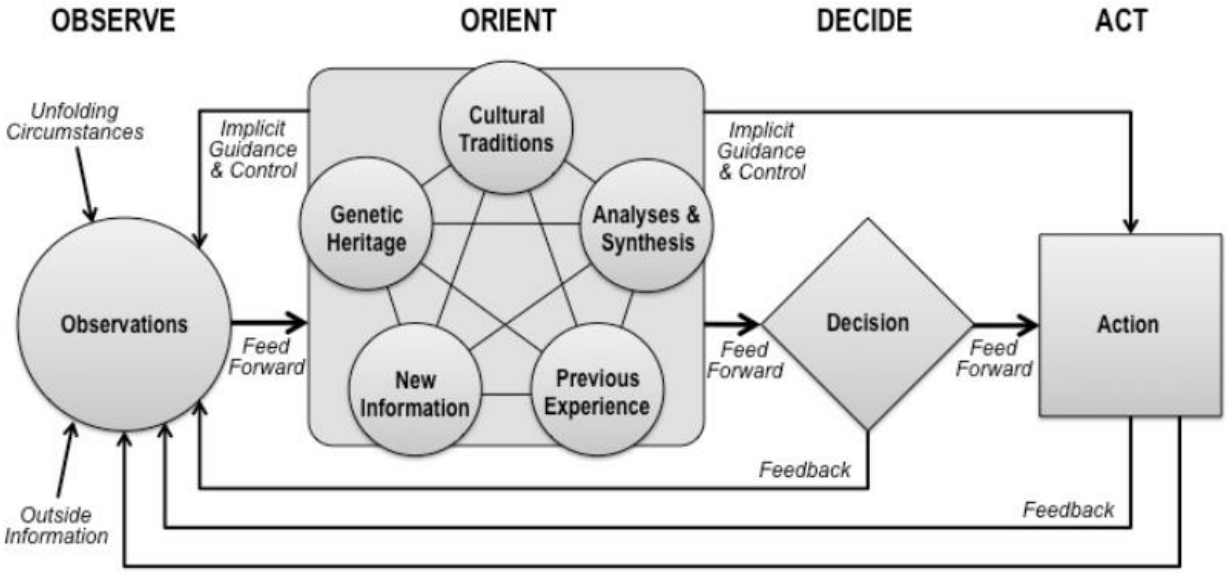

Figure 1 Boyd's Observe-Orient-Decide-Act (OODA) Loop (Source: Boyd (1987), Fadok (1995) and Boyd (1996).

Originally developed for the combat operations process, the OODA loop has been "ascended" to the strategic and tactical levels, not only in the military but also in the business world. Businesses sometimes use it to support the risk management process. The steps of the OODA loop can also be seen in the PP threat assessment. The connecting factors here are "analysis" (orient) and "action" (act).

There are no explicit alternatives to the OODA loop that focus on the deep understanding of how and why people make their decisions. But a few ideas that can be combined with the OODA loop include the following (Hashemi-Pour, 2023):

- **Military decision-making process**. This is another military decision-making method that involves the following seven steps:

Receipt of mission. Mission analysis. Course of action development. Course of action analysis and war gaming. Course of action comparison. Course of action decision. Orders production, dissemination and transition.

- **The plan-do-check-act** (PDCA) **cycle** (or *Shewhart cycle*) is geared toward continuous improvement that consist from four parts. The process starts by identifying a problem and gathering relevant data to the cause of the problem. Then, this information is used to develop and implement a solution. The results are then confirmed or checked before being documented and used to make recommendations for further PDCA cycles.
- **Strengths, weaknesses, opportunities and threats analyse** (SWOT). Businesses use the SWOT framework to identify and analyse any internal or external factors that could affect the success of a project.
- **Getting Things Done method**. This time management model helps organizations break larger projects into smaller, actionable tasks. The Getting Things Done method is a five-step process (collect, process, organize, plan and do).

Like the OODA loop, the SWOT analysis technique has practical value in real-world scenarios.

The essence of Predictive Profiling

PP is a methodology designed to identify, assess and respond to potential criminal or terrorist threats as early as possible. It focuses on the observation of individuals or suspicious behaviour, suspicious objects and/or incidents. PP considers the capabilities of adversaries to attack an organisation or individuals, rather than just the organisation's own capabilities to prevent an attack. It is a proactive technique that aims to identify and disrupt criminal and terrorist activity in its preparatory stages. It can also be applied to recognize and mitigate various other types of threats.

In comparison with *KMar* tasks, such as object security, personal protection, border control, airport policing, etc. PP could be particularly effective in tasks performed by the SBCS as well. To ensure the effective implementation of PP, it is crucial to establish a strong intelligence position. *KMar* additionally notes that PP is predominantly applied in operational environments (Mulder, 2014).

In order to have a clear understanding of the PP methodology, the concepts of Red Teaming, Attacker Method of Operation (AMO),

Assessment, Standard Operating Procedure (SOP), and Security Questioning will be explained.

Red Teaming, within the context of PP, is an operational method of viewing the weak points in the operational security of one's own organization through the eyes of the adversary, as well as testing them. Red Teaming is conducted to improve the quality and execution of security processes by gaining insight into AMOs that criminals or terrorists may potentially use in the future. By attacking one's own organization based on old information combined with new intelligence, potential modes of operation used by attackers can be determined (Zenko, 2015). In this way, visibility is gained into “Known Unknown” information (known adversaries with new AMOs) and "Unknown Unknown" information (unknown adversaries with unknown AMOs), as described in the Rumsfeld matrix (Kroǵerus, 2012).

Based on the results of the red teaming, SOPs can be adjusted and the implementers of the security process can be trained. If red teaming is not systematically employed or of insufficient quality, vulnerabilities may go unnoticed and the effectiveness of implemented measures cannot be properly assessed. Red Teaming plays a leading role in the proactive security cycle; the SBGS therefore needs to encourage the development of such teams.

The Attacker Method of Operation (AMO) provides insight into the actions of criminals, militant activists, terrorists, and other adversaries. This allows security measures to be tailored in terms of level and orientation. AMOs are developed against the backdrop of the Criminal Planning Cycle (Figure 2), which consists of eight steps. Understanding these steps promotes the recognition of potential intentions or actions by wrongdoers against the organization, individuals, or (protected) interests. AMOs can be specific or generic in nature.

When there is a specific and concrete threat, more specific AMOs can be developed. Specific AMOs can be considered as “precise” (specifically targeting that particular group, perpetrator, or group of perpetrators). If the threat is more general in nature (e.g. due to limited availability of concrete intelligence), this will lead to more generic AMOs. Generic AMOs can be seen as “coarse” (broadly applicable to many situations). Indicators for deviant behaviour of an attacker can be derived from an AMO. In the SBGS should be realized that developing and establishing indicators for deviant behaviour is not a straightforward matter, as the indicators can vary for each situation, environment, and circumstance.

Assessment (interpretation) is an extremely important step as it involves a substantive analysis of the threat. The common literature assumes the threat, rather than the risk. The underlying reason for this is

that “risk” can be measured to some extent, while “threat” cannot. Threat either exists or it doesn't, and since the goal is to eliminate the threat (immediately) through intervention, the application of risk thinking is of limited relevance. It may therefore be better to refer to “interpretation” of the threat instead of “assessment”. Indeed, a true assessment generally only occurs when a risk assessment is conducted.

Furthermore, the authors believe that risk thinking can further enhance the strength of PP. It should be applied against the backdrop of risk management. If the security responsible is familiar with the methodology of risk assessment, they will be better able to interpret the threat (in context).

Standard Operating Procedure (SOP). Now that the outcome of the “interpretation” of the threat is known, targeted measures can be taken against the terrorist or criminal group or individuals. Building a strong intelligence position in advance and maintaining it continuously is essential in order to intervene as early as possible. This ideally happens during preparation activities in the earlier stages of the Criminal Planning Cycle.

The intervention (action) is carried out based on a standard operating procedure (SOP). An SOP is a written work instruction that defines responsibilities, tasks, and authorities. The aim is to create uniformity in the execution of the action and therefore in the end result. An SOP can, for example, describe the methods and drills that can be used to neutralize threats by disabling the opponents. An SOP may involve conducting security questioning, making stops, arrests, or using other legal powers. Being able to blindly carry out SOPs and drills in combat situations or other forms of confrontation with the opponents is only possible with frequent practice. Action intelligence is an extremely important prerequisite in this regard.

Security questioning is an operational technique aimed at debunking a perceived threat based on abnormal behaviour. During security questioning, a person is unexpectedly interrogated and asked to explain their displayed abnormal behaviour. The element of surprise enhances the success of this technique. By asking certain uncommon open-ended questions to the individual in question, they are caught off guard. It often becomes difficult for them to provide an immediate truthful response when confronted with their abnormal behaviour. This can lead to a confrontational situation that helps alleviate the threat. However, it should be noted that the threat can also escalate as the individual feels caught and may react with violence out of panic or other reasons. Therefore, addressing the individual should take into account the potential escalation of violence.

If a threat is not debunked through the application of security questioning, immediate action is taken based on a standard operating procedure (SOP).

PP starts with the observation of deviations from the norm based on visible behaviour of individuals. If these deviations can be linked to an AMO, then a threat is recognized. The Police/ SBGS then take action in accordance with the SOP. This may involve security questioning, detaining, arresting, or utilizing other legal authorities. Establishing the norm and indicators of abnormal behaviour is informed by intelligence. Linking visible abnormal behaviour to intelligence helps prevent discrimination and profiling based on ethnicity.

The work process of a criminal or terrorist is described in the criminal terrorist planning cycle (or Attack Cycle). This cycle consists of seven steps (LaFree, Freilich, 2016):

1. Preliminary target selection;
2. Gathering information/ Initial Surveillance. Exploring the target / Final target Selection;
3. Planning and coordinating the different aspects/ Pre attack Surveillance/ Gathering the necessary materials (tooling up);
4. Performing a rehearsal (dry run);
5. Carrying out the attack/ Execution;
6. Escape & (excluding suicide bombers);
7. Exploitation.

Due to these steps are not all visible in the physical world, intelligence is of great importance for a secure organization and its security personnel.

In the digital world, visibility exists in step 2, particularly through digital investigation to search for indicators in the field of Open Sources Intelligence (OSINT). In step 5 of the planning cycle, the criminal or terrorist may also be visible. They may be visible to the organization being attacked or to agencies from which the criminal or terrorist obtains their needed materials. This can include trading companies dealing with, for example, raw materials for Home Made Explosives. Within steps 3, 6 and 7, the Police/ SBGS may, in all tasks, encounter physical behaviour that deviates from the norm.

To apply PP, it is essential to identify suspicious indicators. These indicators are determined in the intelligence process based on known Means, Motive, and Opportunity (AMO's). To make security even more proactive, it is also important to gain insight into AMO's that may be used in the future. PP also offers a possibility for this by going through the Proactive Security Cycle in which the Red Teaming tool plays a leading role.

Within this Proactive Security Cycle, the aim is to examine the weaknesses in the operational security of our own organization from the perspective of the adversary, using red teaming, and to test them. It also includes the execution of alternative hypotheses and the simulation of existing SOPs and processes. All of this is done to improve the quality and

implementation of security processes by identifying possible future AMOs that could be used by criminals or terrorists. By testing our own organization, potential modus operandi of attackers can be determined, SOPs can be adjusted, and the performers of the security process can be trained. This process is a self-repeating system that never stops and is focused on continuous quality improvement (Mulder, 2014).

There may be a misunderstanding about the relationship between PP and risk assessment and when PP should be used instead of risk assessment in a particular situation. The following will delve into this relationship, the differences, and when the added value of both is most effective.

The bowtie method is a visual way of understanding the impacts of a hazard, the risk it presents, the consequences and the controls that should be put in place (De Ruijter & Guldenmund, 2016). The bowtie has become popular as a structured method to assess risk where a quantitive approach is not possible or desirable. The success of the diagram is that it is simple and easy for the non- specialist to understand. The idea is a simple one of combining the cause and the consequence. When the fault tree is drawn on the left hand side and the event tree is drawn on the right hand side with the hazard drawn as a "knot" in the middle the diagram looks a bit like a bowtie. This method of analysis uses the risk matrix to categorise the various scenarios, and then carries out analysis on those with the highest risks. The essence is to establish how many safety barriers there are available to prevent, control or mitigate the identified scenarios, and the quality of those barriers.

Risk is defined as the Combination of Probability and Consequence. An excellent way of estimating the risk is to use a Risk Matrix (BowTie Pro™, 2024).

The threats and consequences are managed by the combination of the controls. Each control is a barrier where the combination of the controls should eliminate the hazard or reduce its frequency of occurrence, or mitigate its potential consequences. It is only when all the controls fail that the hazard or consequence will occur depending on which side of the bowtie you are working, described by James Reason as the "Swiss cheese model" (or "cumulative act effect"). The controls can include physical or operational systems and procedures that may be in place. In many cases it is better to use a more pragmatic approach with rigorous peer review.

There is a rule that the system should be "ALARP" ("As Low As Reasonably Practicable"). At the core is the concept of "reasonably practicable"; this involves weighing a risk against the trouble, time and money needed to control it. Thus, ALARP describes the level to which we expect to see workplace risks controlled.

The authors devote additional attention to the analysis of the level of staff security. In 1995, following the Chornobyl disaster, Vernon Bradley developed “DuPont Bradley Curve Model”. It describes the relationship between incident rate and the organization's behaviour. Five years later, a Dr. Patrick Hudson proposed “Safety culture maturity model”. In the Hudson model, there was a more in-depth analysis focused on the level of the employee and how they could be impacted by the company safety culture – or lack thereof.

This model framework establishes five stages of maturity (Pathological; Reactive; Calculative; Proactive and Generative). These five stages of safety culture demonstrate the level of commitment felt by the workers and managers towards safety. Furthermore, it reveals the degree of trust employees have in their leaders and managers. These studies are conducted by survey questions (conducted anonymously in the company by survey forms) to employees and leadership at all levels. Often these studies also include focus groups to dig further into the results to gain more clarity. Most companies, no matter where you are, will have safety management systems in place to ensure that they are compliant with country or corporate regulations. So this puts many companies somewhere between Reactive and Calculative in their approach to safety. But the challenge is to get further up the ladder and this is where demonstrable Leadership commitment becomes the key to success (Hudson, 2001).

According to KMar's research, PP is based on threat analysis and its interpretation and almost always relates to operational matters (operational level). However, if one is in the early stages of the criminal planning cycle and a specific AMO has already been established, thus allowing more time for the application of PP, PP can take on tactical elements. It is observed that risk assessment is mainly applied at the tactical and strategic levels. In general, there is more time at these levels to carry out a more comprehensive security assessment than in an operational situation. The criminal planning cycle can be better explored and understood, and the potential impact can be better determined, if a risk assessment is carried out.

It can be concluded that the application and results of PP are strengthened when combined with risk thinking. Risk assessment, when applied at the operational level, is enhanced by looking at deviations from the normal behaviour of individuals. Conversely, security personnel will be better able to interpret the threat if they are familiar with the methodology of risk assessment.

It is important to note that PP is an offensive security technique that focuses on the behaviour of individuals, whereas risk assessment is a more defensive security technique that focuses on the broad spectrum of "assets".

These include people, property, interests, objects and intangible assets such as reputation and integrity. The scope of risk assessment is therefore much broader than that of PP and aims to improve resilience. PP reverses the roles and takes the initiative away from the adversary. PP is therefore much more focused on intervention.

Conclusions and suggestions

The above aims to provide insight into when KMar use risk assessment or when use PP in a specific situation. There is some overlap between both tools, especially when PP takes on a tactical dimension in an extensive analysis of the criminal planning cycle and in specific AMOs.

The authors agree with KMar's conclusions that both tools are complementary and can reinforce each other. In practice, both tools can be used alongside each other, depending on the situation and the amount of time available – tailored to the specific circumstances.

The authors believe that it is necessary for the SBGS to look into the implementation of the methods described in the paper.

References

1. Azuma, R., Daily, M., & Furmanski, C. (2006). A review of time-critical decision-making models and human cognitive processes. *2006 IEEE Aerospace Conference Proceedings*, Big Sky, MT, USA.
2. Blaha, L. M. (2018). *Interactive OODA processes for operational joint human-machine intelligence*. NATO Science and Technology Organization (STO).
3. Boyd, J. R. (1987). *Organic design for command and control*. In *A discourse on winning and losing*. Maxwell Air Force Base, AL: Air University Press.
4. Boyd, J. R. (1996). *The essence of winning and losing*. Unpublished lecture notes. Maxwell Air Force Base, AL.
5. Boyd, J. R. (2018). *A discourse on winning and losing*. Maxwell Air Force Base, AL: Air University Press.
6. De Ruijter, A., & Guldenmund, F. (2016). The Bowtie method: A review. *Safety Science, 88*, 211–218. https://doi.org/10.1016/j.ssci.2016.03.001
7. Fadok, D. S. (1995). *John Boyd and John Warden: Air Power's quest for strategic paralysis*. Maxwell Air Force Base, AL: School of Advanced Airpower Studies, Air University.
8. Hashemi-Pour, C. (2023). What is the OODA loop? *TechTarget*. Retrieved from https://www.techtarget.com/searchcio/definition/OODA-loop
9. Krogerus, M., & Tschäppeler, R. (2012). *The decision book: 50 models for strategic thinking*. New York, NY: W. W. Norton & Company.
10. LaFree, G., & Freilich, J. D. (2016). *The handbook of the criminology of terrorism*. Hoboken, NJ: Wiley-Blackwell.
11. Mulder, P. (2014). *Predictive profiling terrorism*.
12. Reason, J. (1990). The contribution of latent human failures to the breakdown of complex systems. *Philosophical Transactions of the Royal Society of London. Series*

B, Biological Sciences, 327(1241), 475–484. https://doi.org/10.1098/rstb.1990.0090
13. Staff, T. (2021). 35 years after El Al bomb plot, security staff recount stopping unwitting bomber. *The Times of Israel*. Retrieved from https://www.timesofisrael.com/35-years-after-el-al-bomb-plot-security-staff-recount-stopping-unwitting-bomber/
14. TorchStone. (2022). The importance of understanding the attack cycle. *TorchStone Global*. Retrieved from https://www.torchstoneglobal.com/the-importance-of-understanding-the-attack-cycle/
15. Zenko, M. (2015). *Red team: How to succeed by thinking like the enemy*. New York, NY: Basic Books.