World Journal of Information Systems 2(3) 11-26
DOI: https://doi.org/10.17013/wjis.v2i3.40

Article

Evolving Threat Landscapes: A Multi-faceted Diagnosis Model for Countering Digital-Age Menaces to Vulnerable Targets

Sónia M. A. Morgado [1,2], Margarida Carvalho [1,2] and Sérgio Felgueiras [1,2]

[1] Research Center (ICPOL), Lisbon, Portugal

[2] Instituto Superior de Ciências Policiais e Segurança Interna, Lisbon, Portugal

***** Correspondence: smmorgado@iscpsi.pt

(Article history: Received June 25, 2025; Received in revised form July 18, 2025; Accepted August 19, 2025; Available online September 15, 2025)

Abstract: In an era of increasing digital interconnectedness, the vulnerability of public spaces—or 'soft targets'—has expanded from the physical to the digital realm, giving rise to the complex phenomenon of the 'e-threat'. Traditional security paradigms are often ill-equipped to address these diffuse, data-driven menaces that exploit the convergence of our online and offline lives. This paper introduces a multi-faceted diagnostic model designed to navigate this evolving landscape. Our framework is built upon the critical triangulation of three interconnected planes: a theoretical plane that conceptualizes the nature of modern threats; an empirical plane that leverages artificial intelligence and advanced data analytics for proactive detection; and a crucial normative plane that embeds ethical principles, human rights, and legal frameworks at the core of any technological application. By analysing the tension between technological capabilities and societal values — drawing on real-world initiatives like the APPRAISE Project with MARPLE — this work argues that effective security is not a zero-sum game. Ultimately, the model demonstrates that safeguarding soft targets against digital-age menaces requires a holistic synergy between technological innovation and an unwavering commitment to democratic governance and the Sustainable Development Goals, ensuring a future that is both safe and free.

Keywords: e-threats; soft targets; proactive policing; artificial intelligence; diagnosis model; ethical governance; security and safety; sustainable development goals

© 2025 ITMA. All rights reserved.

1. Introduction

In an era of evolving threat landscapes, the seemingly straightforward notion of a threat—a person or group intending to harm vulnerable "soft targets"—has become profoundly more complex. The key questions of "who," "what," and "how" are no longer confined to the physical world. The digital age, characterized by the internet, the Internet of Things (IoT), big data, and artificial intelligence, has introduced new mechanisms for processing communication, targeting victims based on frequency, intensity, and vulnerability, and employing a range of human, technical, and weaponized tools to achieve malicious ends. This technological revolution has fundamentally impacted the definition of threats, shifting the focus to activities within cyberspace and expanding the concept from traditional threats to "e-threats" and the complex task of assessing their associated risks.

The systematic discussion of threat assessment dates to the 19th century [1]and has since been developed by numerous authors throughout the 20th century [2-5]and into the present day [6-7]. A central tenet across all these conceptualizations is the critical need to identify warning behaviours that signal an increasing or accelerating risk of a threat [7]. Regardless of whether the threat is traditional or a digital e-threat, each requires a continuous, dynamic process of designing and implementing a risk diagnosis model [8]. In our contemporary world, the critical nature of cyberspace and the clandestine actions used to perpetrate crimes or terrorist attacks necessitate new models for determining and diagnosing these e-threats.

Today, cyberspace, or e-space, represents a new dimension of the public square, reshaping security needs [8]. Advanced technologies, as sophisticated and decentralized tools, can be used by states, organizations, or individuals to help mitigate the negative impacts of these newly emerging threat forms. On one hand, they provide knowledge and benefits that assist security forces and other safety providers. On the other hand, their constantly changing, ambiguous, and multifaceted nature creates pathways for a vast universe of criminal and deviant behaviours, which translate into threats and are quantified as risks. This has led to a clear trend of threats migrating to the cyber network, effectively "causing the displacement of the battlefield to cyberspace" (p. 32) [9]. This migration inevitably exponentiates the risk of cybercrime, as the World Economic Forum [10] notes: “as society continues to migrate into the digital world, the threat of cybercrime looms large” (p.46).

The threats emerging from this network are produced by diverse, often unidentified, and disguised actors. They can operate across a global geography, bypassing physical state borders. Within this universe, a criminal can access a vast number of potential victims, conceal their identity, and orchestrate illicit activities on an unprecedented scale. Europol [11] warns that this type of crime is set to skyrocket, stating, “In light of these developments, the market for criminal goods and services is booming,” which calls for a unified and objective response that begins with detection (p. 8).

The research philosophy underpinning this theoretical paper is grounded in peer-reviewed literature, supplemented by grey literature from sources such as the European Data

© 2025 ITMA. All rights reserved.

Protection Board (EDPB), the European Data Protection Supervisor (EDPS), the European Commission, and the United Nations Interregional Crime and Justice Research Institute (UNICRI). The peer-reviewed literature was sourced from comprehensive databases including EBSCO, Scopus, Science-Direct, Google Scholar, B-on, and RCAAP. Documents were excluded if they offered no added value, were irrelevant to the main topic, were of poor quality, or were working papers, posters, dissertations, or abstracts, to maintain the integrity of the paper. The paper argues that an effective diagnosis model for e-threats requires the triangulation of empirical data from technology, a solid theoretical understanding of threat evolution, and a robust normative framework to ensure that proactive policing strategies safeguard fundamental human rights.

2. State of the art

A foundational responsibility of any government is the provision of national security. In this capacity, the state provides safety and security, which are considered public goods because they are both non-rivalrous (inexhaustible) and non-excludable. Law enforcement agencies are therefore indispensable for upholding this role by protecting society from the descent into anarchy, anomy (normlessness), and social unrest. Effective police leadership is essential to guide these agencies through evolving challenges [12]. Although multiple agencies hold mandates for social regulation, the objective of societal protection requires law enforcement to implement efficient, proactive, and predictive policing strategies. This need for efficiency is particularly critical in complex domains such as securing soft targets within the contemporary digital landscape. The transformative power of artificial intelligence is creating a paradigm shift in how security is conceptualized and delivered [13].

2.1. Soft -targets

The intrinsic vulnerabilities of soft targets have necessitated a focused effort from the security sector to enhance their protection. A key definition is provided by the European Commission, which considers a soft target as locations that “are vulnerable and difficult to protect and are also characterised by a high probability of mass casualties in the event of an attack” (p. 4) [14].

A significant challenge in this domain is the conceptual ambiguity surrounding the term "soft target." Despite numerous scholarly contributions, a consensus on a single, operational definition remains elusive, partly because the term can be applied to various types of targets. This definitional variance limits its practical application, a critique articulated by Zeman [15], who notes that existing “definitions are very common, which does not allow their use in the process of soft targets identification” (p. 109)

The absence of a single, official definition for the term is a noted issue; as Kalvach et al. [16] state, “there is no official definition for the term ‘soft targets’” (p. 6). Nevertheless, a common operational definition has emerged within security practice which identifies such

© 2025 ITMA. All rights reserved.

locations as attractive to terrorists due to a combination of high population density and minimal security measures. This characterization is supported by Beňová et al. [17], who state that “soft targets are characterised as places with a high concentration of people and low level of security” (p. 2).

Notwithstanding the theoretical debate, a review of various proposals indicates several common features defining a soft target. Large sporting events provide a concrete example, as their high concentration of attendees in an open environment necessitates specific policing strategies environment [18]. To operationalize this concept, the present analysis adopts the definition from Schmid [19], who considers that “soft targets are undefended and/or under-protected open access locations with low, or no security provided where civilians can be found in significant numbers” (p. 818).

A prevailing approach to securing soft targets involves implementing heightened security measures, a strategy that can paradoxically alter the fundamental nature of the location itself. This transformation process may be interpreted as a tactical success for terrorist objectives, as the disruption of the space's normative function and character is, in itself, a desired outcome. This fundamental tension between security imperatives and civil liberties was acutely demonstrated during the COVID-19 pandemic, where police actions had to navigate public health crises while respecting fundamental rights [20]. Furthermore, comprehensively "hardening" all soft targets is not a viable strategy due to its logistical infeasibility and profound societal costs. Even if such a transformation were possible, it would fundamentally alter daily life and severely curtail the exercise of fundamental rights, creating a closed-off society at odds with democratic principles. This challenge directly aligns with the United Nations' Sustainable Development Goals (SDGs) [21], particularly SDG 11 (Sustainable Cities and Communities), which seeks to ensure public access to safe, inclusive, and accessible green and public spaces, and SDG 16 (Peace, Justice and Strong Institutions), which aims to significantly reduce all forms of violence and related death rates. Protecting soft targets is therefore not just a matter of national security, but a prerequisite for building peaceful, just, and sustainable societies.

Therefore, modern strategies are shifting towards a multi-layered approach that integrates technology and collaboration. This includes the development of new technological tools, such as body-worn cameras [22], and reflects a broader evolution in how technology is adopted within policing [23]. Projects such as APPRAISE aim to facilitate cooperation between public and private security operators to mitigate terrorist scenarios [24], while initiatives like MARPLE focus on using AI-driven systems for threat detection and response to better secure soft targets [25].

The persistence of the terrorist threat in Europe, marked by attacks across multiple members states, remains a significant security concern. This reality is quantified in the Europol TE-SAT report [26], which states that “terrorism remains a key threat to the internal security of the EU. Fifteen completed, foiled and failed terrorist attacks were recorded in the EU in 2021. The four completed attacks included three jihadist terrorist attacks and one left-

© 2025 ITMA. All rights reserved.

wing terrorist attack" (p. 3). In analysing these events, it is critical to recognize the facilitating role of the digital domain. The same report [26] underscores this connection, noting that "the online environment plays a key role in this as it facilitates (self-)radicalisation and the spread of terrorist propaganda. Europol has significantly scaled up its capabilities in identifying terrorist and violent extremist content and is working with online providers to remove it" (p. 3).

This physical threat is increasingly intertwined with the digital world. The very characteristics that make a location a "soft target"—accessibility, high traffic, and symbolic value—are now being exploited through a new vector: cyberspace. This digital domain acts as an accelerator, a space where ideologies of hate can be cultivated and translated into real-world violence against these vulnerable locations. The challenge of securing soft targets is therefore no longer confined to physical measures alone; it is now intrinsically linked to the digital ecosystem that can inspire and enable attacks. Achieving the sustainable development goal of safe and inclusive public spaces (SDG 11) is impossible without addressing the online-to-offline threat pipeline. The failure to secure the digital environment directly undermines the safety of the physical one, creating a vicious cycle where online radicalization can lead to tragic outcomes at undefended public gatherings. It is within this new reality that the concept of the "e-threat" emerges as a critical area of focus for modern security and intelligence efforts.

2.2. e -threats

The global pandemic period served as a significant catalyst, accelerating the migration of social and professional life into cyberspace. This digital shift, however, was accompanied by a noticeable increase in deviant online activities, a trend particularly visible among younger people. The unique pressures of this era created new challenges for public security, forcing a re-evaluation of the balance between state authority and individual freedoms in a crisis [20]. The TE-SAT report [27] elaborated on the pandemic's impact, stating:

> "the combination of social isolation and more time spent online during the pandemic has exacerbated the risks posed by violent extremist propaganda and terrorist content online, particularly among younger people and minors. Gaming platforms and services are increasingly used by right-wing terrorists to channel terrorist propaganda targeting a younger generation of users. Pandemic-linked restrictions also have the potential to exacerbate pre-existing mental health issues potentially prompting violent acts that resemble terrorist or violent extremist attacks (p. 5)."

A direct correlation between cyberspace activity and real-world terrorist attacks is now clearly established in TE-SAT reports [26]. These findings indicate that physical attacks are frequently preceded by a range of online preparatory actions, such as recruitment, training, self-indoctrination, the fostering of radicalization, and the procurement of weapons or explosives [26]. The preparatory phase in cyberspace often includes recruiting and

© 2025 ITMA. All rights reserved.

connecting new activists, facilitating training, and acquiring resources. On this, the TE-SAT 2022 report specifies that “Online community building often plays a key role, as it connects peers virtually on a global scale. This drives radicalisation and provides access to terrorist propaganda, instructional material and opportunities for procurement of weapons and explosives precursors” (p. 30) [26].

Therefore, identifying e-threats is now a critical component of preventing attacks against soft targets. To do so requires a precise definition of the term. A United Nations [27] report offers a broad understanding of a threat as “any event or process that leads to large-scale death or lessening of life chances and undermines States as the basic unit of the international system (...)” (p. 24). This notion of imminent danger, which Creppel [28] described as being as palpable as a "house on fire," is now understood to exist across "physical threats, economic threats and cyber threats" (p.156) [29]. Consequently, the very concept of a threat has been adapted to the digital dimension, where it is termed a cyber threat or e-threat.

Within this paper, an e-threat is conceived as any factor, event, or action in cyberspace that has the potential to “cause damage to the integrity of people, beings or things” (p. 1168) [30], whether that damage is material or moral. These threats manifest across a spectrum, from “social intervention ("cyber-activism", "cyber-hacktivism", "cyber-vandalism", or "cyber-graffiti")” to “criminal actions (hacking, cracking, cybercrime or cyber-terrorism), or even the form of acts of war (cyber-warfare)” [31]. The motivations are equally varied, often revolving around “egoism, anarchy, money, destruction and power” [29] (p. 159). This extends beyond terrorism to include the activities of organized crime, which leverages online platforms and media for recruitment and normalization of criminal enterprise [32]. Crucially, the definition of an e-threat remains a social construction, dependent on the actor who chooses to frame an issue as an existential danger.

The inherent uncertainty and non-knowledge [33] surrounding modern crime necessitate innovative prevention strategies. This is especially true for e-threats, which lack the physical indicators present in traditional threat assessment. For instance, a study by Eachus et al. [34] identified stress as a crucial element for detecting hostile intent in crowded physical spaces, where it produces observable biological and psychological signs. In cyberspace, the criminal is an invisible actor, making such physical detection impossible. This digital shift demands a corresponding evolution in law enforcement, requiring modern police leadership capable of navigating technological complexities [12] and a strategic adoption of new technologies [23]. The diagnosis of e-threats must therefore rely on analyzing a user's digital conduct—their communications, activities, and online footprint.

Social networks are a primary arena for such analysis. In our interconnected network society [35], the sheer volume of users has amplified the spread of offensive and dangerous speech. It has been observed that “social media by definition can be viewed as a potential accelerator for hate speech in uncontrolled contexts” (p. 161) [36]. Hate speech, defined by Khan et al. [37] as words that are "hurtful towards a person or a group of people on the basis of race, caste, gender, colour, ethnicity and also support and promote violence against the

© 2025 ITMA. All rights reserved.

targeted groups" (p. 688), directly undermines the aims of SDG 16 (Peace, Justice and Strong Institutions) by promoting violence and threatening public safety. By targeting specific groups, it also works against SDG 10 (Reduced Inequalities). This online vitriol is not an abstract problem; it is a direct precursor to violence that can manifest at soft targets like schools, places of worship, and public markets.

To counter this, a new generation of tools is required. The work of Mussiraliyeva et al. [38] in detecting online radicalization on Twitter showed that linguistic analysis can serve as an "informative predictor of the user's fundamental interests" (p.2). This represents the transformative potential of artificial intelligence, which is causing a metamorphosis in security paradigms [13]. Likewise, a study by Aziz et al. [39] on detecting racist content via keywords highlights the importance of monitoring cyber communication. These examples show that it is possible to recognize e-threats by leveraging AI and machine learning, forming the basis for advanced detection systems like those being developed in the MARPLE project [25]. Beyond just detection, technology can also play a role in public health and prevention, as seen in the development of tools like the AinoAid chatbot to address issues such as domestic violence, which shares underlying social drivers with other forms of aggression [40]. This holistic approach, which combines technological enforcement with social prevention, is essential for creating truly safe communities.

In cyberspace, a user's digital activity presents a diagnostic avenue for e-threats that complements the analysis of speech. A prime example is the trail of data, or "digital footprint," created through content consumption and e-commerce on major platforms such as Youtube, Google, Yahoo, and Amazon. These platforms have both the access and the opportunity to monitor these actions. While web services are primarily motivated by commercial interests in this tracking [41], the resulting information is crucial for authorities. It can be used to identify hostile intentions by analyzing patterns in the goods, services, or content an internet user engages with. The significance of this digital footprint is underscored by the fact that the *modus operandi* for many illicit acts includes online preparatory steps. For example, "the planning and preparation of attacks were frequently accompanied by auxiliary offences such as self-training, including the exchange of tactical information online" (p. 26) [26]. This activity allows for a screening to occur in the "pre-crime phase" (p. 491) [423]. Therefore, within the cyber dimension, threat detection is necessarily confined to analyzing conduct as revealed through speech and digital activities, making it an exceptionally complex issue.

3. Perspectives and Directions

Reflection on the protection of soft targets must prioritize the anticipation of threat identification processes, shifting from a reactive to a proactive stance. This is particularly urgent for e-threats, given their direct relationship with attacks on vulnerable public spaces, such as large sporting events which require complex, multi-layered security approaches [18].

© 2025 ITMA. All rights reserved.

The primary work must therefore focus on detecting the early, often subtle, signs that indicate an intent to perpetrate an attack, with a specific emphasis on identifying preparatory acts.

However, the difficulty in identifying e-threats stems from several complex factors, making the process akin to searching for a needle in a digital haystack. The first barrier is the sheer volume of daily events occurring in soft targets and online, which, when combined with limited resources and the constraints of bounded rationality, makes an exhaustive analysis of every event unfeasible. Within cyberspace, information linked to an e-threat often exists as disconnected fragments that require intensive study to construct an intelligible picture for security managers. These fragments are frequently encrypted or obscured through coded language, which facilitates their camouflage. A third aspect is the inherent complexity of terrorist plots, which are initiated through preparatory acts. Detecting these preliminary steps may not guarantee the prevention of subsequent actions, and for this reason, the process of analysing disparate data and information is often fraught with uncertainty.

The application of digital tools to identify e-threats represents a significant leap forward. This technological shift, however, requires new forms of agile and informed police leadership capable of navigating both the strategic implementation of new systems and their ethical implications [12]. The exponential increase in the amount of data that can be analysed, a marked decrease in research time, the use of models allowing for data triangulation, the creation of historical e-threat databases, and the identification of patterns from past terrorist attacks all serve to boost the intelligence effort by mitigating the limitations of bounded rationality. Despite these clear advantages, the profound societal, ethical, legal, and privacy constraints must remain at the forefront of any implementation.

The development of analysis models composed of criteria and rules to identify the technical indicators of an e-threat must be a priority for states, international organizations, and the global community. This requires a multidisciplinary effort, uniting technical experts, legal advisors, and security specialists. This collaborative philosophy is embodied in research initiatives like the APPRAISE project, which focuses on facilitating cooperation between public and private security operators to mitigate terrorist scenarios [24]. The digitalization of these models, including the deployment of advanced AI as explored in the MARPLE project [25], is a key priority. However, the confidentiality surrounding the construction of these advanced detection tools often poses a further barrier to the necessary cooperation processes.

To lay the groundwork for a viable diagnostic model, the preliminary considerations must be analysed across three interconnected planes: the theoretical, the empirical, and the normative.

Delivering intelligence through the analysis of elements gathered with a suite of hi-tech tools allows for a deeper understanding of social media's ubiquity as an open source of information [43, 44]. As globalization continues to shrink geographic, cultural, and social distances [45], the same process has made criminal and terrorist networks more borderless, leveraging technology for both their operations and the detection of their e-threats. The recognition that e-threat detection is vital for intelligence development means that embracing

© 2025 ITMA. All rights reserved.

technology in objective-driven policing is a critical resource for every security force [46]. In this challenging and evolving world of geo-globalization and geo-e-threats, protecting critical assets and soft targets necessitates the application of the 4Ps: Prevention, Proactivity, Predictively, and Patterns [47]. Prevention itself is a multi-faceted concept, extending beyond detection to include public awareness and communication, using strategies of emotional engagement like those proven effective in other domains like road safety [48].

The 4Ps are only manageable if law enforcement and intelligence services can apply the latest technologies—such as Body-Worn Cameras [22], augmented reality, blockchain, AI, the Internet of Things (IoT), and Facial Recognition Technology (FRT)—fundamentally altering the landscape of police action. This integration offers the possibility, even in a chaotic environment, to provide law enforcement with the means to predict, analyse, recognize, and communicate threats, thereby increasing their accountability and transparency [49]. This transformative potential of artificial intelligence is creating a genuine metamorphosis in security paradigms [13].

However, this technological road must be navigated with caution. It demands a triangulation of algorithms and interoperability between all stakeholders to enhance benefits and mitigate risks, which include threats to Fundamental Human Rights, the misuse of technology by criminal and terrorist groups, and even risks to human survival [50]. This is where the normative framework becomes paramount, not as a barrier, but as a guiding principle to ensure security initiatives align with the goals of SDG 16 (Peace, Justice, and Strong Institutions). Exploring the architecture of these challenges reveals that the normative basis involves profound questions of Fundamental Human Rights, freedom of speech, personal data protection, privacy, and ethics [51-55]. The intricate balance between law, regulation, and technology directly affects human rights, as the sacredness of human life remains the core idea [56].

The intersection of technology and e-threat detection is most pronounced in the areas of privacy and data protection, as enshrined in Articles 7 and 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms [57]. While public security bodies have specific exemptions, their intertwined relationship with private security contractors necessitates a clear framework to prevent the violation of fundamental rights when using technological tools [58, 59]. A modern democratic society is inextricably linked with the protection of guaranteed human rights. The EU Directive 95/46/EC [60] and its successors like the GDPR codify principles for managing personal data, defining "processing" as a comprehensive set of operations from collection to destruction [61]. The lawful processing for a specific, legitimate purpose is required, even with the exemptions granted to competent authorities under instruments like the Police Directive [62].

The ultimate challenge lies in avoiding the embedded unfairness of algorithmic decision-making and the biases inherent in human decisions. Trustworthy AI must be lawful, ethical, and robust [63], complying with principles of respect for human autonomy, harm prevention, fairness, and explicability [64]. The European Commission’s ALTAI checklist provides a

© 2025 ITMA. All rights reserved.

practical guide for applying these ethics in both the design and deployment phases of AI systems [65]. The data used must be representative and non-biased to ensure a non-discriminatory agenda. If these principles are not upheld, high-tech advances risk becoming skewed for inequity [66] rather than democratizing human rights. Therefore, a robust normative framework is fundamental to guarantee that e-threat detection technology protects soft targets without compromising individual rights.

From an empirical perspective, concerns about technology's fallibility are significant. While AI has progressed from machine learning to deep learning, the effectiveness of threat detection methodologies still depends heavily on hyper-parameter configurations [67, 68]. These metrics are crucial for building diagnostic models that bridge data collection with decision-making. Yet, an over-reliance on technology can provoke questions about its efficiency versus the ineffectiveness of pondering individuality [69]. The disadvantages are clear: high error susceptibility, the potential for misuse leading to flawed analysis, and the biases of the individuals who create the algorithms [70-72]. As globalization accelerates the spread of both beneficial and dangerous technologies [73], the use of these tools by police rightly invites inquiries into legitimacy and public trust.

The theoretical evolution is thus a transition from assessing the threat a crowd poses to public order, to a dynamic risk assessment of an external threat that may fall upon that crowd. Even with the positive side effects of machine learning and AI, special attention must be paid to their disruptive effects. Siding with Beridze [74], this means that governance and international frameworks must evolve in step with technology to safeguard rights and maintain public trust. The triangulation of the theoretical, empirical, and normative approaches is therefore essential to avoid false positives, combat disinformation, and overcome nuanced problems in discourse analysis. Ultimately, interoperability is the key to creating strategies that minimize the risks of technology in high-stakes decision-making [75]. In light of these considerations, a first approach for a diagnostic model is possible to draw, as shown in Fig. 1.

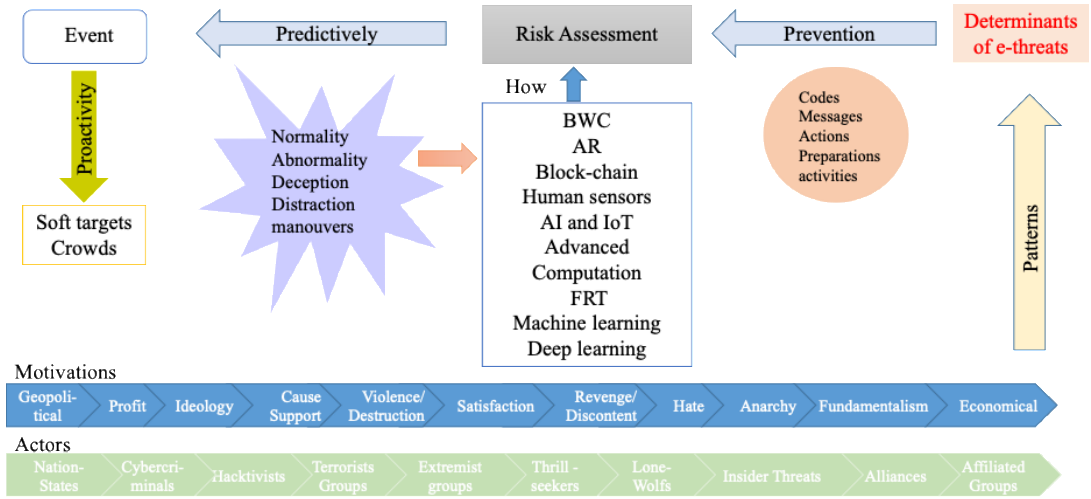


Figure 1. Reproduced under terms of the CC-BY license. Copyright 2024, S. M. A. Morgado, M. Carvalho, M., & S. Felgueiras, Springer.

© 2025 ITMA. All rights reserved.

3. Conclusion

The confluence of desire and expectation forming intent, with the resources and knowledge that build capacity, has found a new and potent medium for expression in cyberspace. This manifestation has given rise to the contemporary formulation of threat: the e-threat. In the digital age, confronting this challenge requires more than just adapting old methods; it demands a fundamental shift in our approach to security, risk, and governance.

The cornerstone of this new approach is the triangulation of the empirical, theoretical, and normative frameworks While advanced mathematical algorithms and AI systems offer unprecedented efficiency in processing vast amounts of information to identify deviant discourse, their outputs are not infallible. Human interaction, particularly the critical evaluation by law enforcement officers, remains indispensable for ensuring the contextual accuracy, relevance, and safety of security decisions. It is this synergy—between technological capability and human oversight—that allows for the effective and equitable management of information. This integrated process increases the validity of intelligence, guarantees good governance, and enables the development of proactive and predictive policing strategies that are truly adequate to the defined risk.

This strategy is not merely a technical exercise; it is a direct contribution to achieving key global mandates outlined in the Sustainable Development Goals. By striving to protect soft targets from both physical and digital threats, this model actively works towards SDG 11 (Sustainable Cities and Communities), ensuring public spaces remain safe and accessible, and SDG 16 (Peace, Justice and Strong Institutions), by reducing violence and building effective, accountable institutions. The shift from theory to practice is already underway, embodied in collaborative initiatives like the APPRAISE project, which unites public and private security actors, and the technological innovation of projects like MARPLE, which leverages AI-driven detection to secure vulnerable locations. These projects represent the tangible application of the principles discussed, demonstrating a forward-looking commitment to protecting citizens.

Ultimately, integrating the risk assessment of e-threats with advanced technology to counter crime and terrorism against soft targets requires a multi-level enactment that thoughtfully manages the interaction with citizens. The pursuit of predictive and proactive policing must be inextricably linked to the safeguarding of human rights and the core social, ethical, and legal principles of a democratic society. The goal is to foster an environment of enhanced awareness and security where the protection of the community does not come at the cost of individual liberty, but rather, reinforces the foundations of a society that is both safe and free.

© 2025 ITMA. All rights reserved.

Acknowledgments: The authors acknowledge the institutional support of the Research Centre of the Instituto Superior de Ciências Policiais e Segurança Interna (CI-ISCPSI / ICPOL). This work was financed by national funds through the FCT – Fundação para a Ciência e a Tecnologia, the Portuguese Foundation for Science and Technology.

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] Laschi, M.; Lombroso, C. Le délit politique. In Actes du Premier Congrès International d'Anthropologie Criminelle, Proceedings of the Premier Congrès International d'Anthropologie Criminelle, Rome, Italy, 1885; Bocca Fréres: Turin, Italy, 1886; pp. 379–389.

[2] Calhoun, T.; Weston, S. *Contemporary threat management*. Specialized Training Services: San Diego, CA, USA, 2003.

[3] Dietz, P.E.; Martell, D. *Mentally disordered offenders in pursuit of celebrities and politicians*. National Institute of Justice: Washington, DC, USA, 1989.

[4] Fein, R.; Vossekuil, B. Assassination in the United States: an operational study of recent assassins, attackers, and near-lethal approachers. *J Forensic Sci* 1999, *44*, 321–333. https://doi.org/10.1520/JFS14457J

[5] Fein, R.; Vossekuil, B.; Holden, G. *Threat assessment: An approach to prevent targeted violence* (NCJ 155000). U.S. Dept. of Justice, Office of Justice Programs, National Institute of Justice: Washington, DC, USA, 1995.

[6] Dietz, P.E.; Martell, D. Commentary: approaching and stalking public figures—a prerequisite to attack. *J Am Acad Psychiatry Law* 2010, *38* (3), 341–348.

[7] Meloy, J.R.; Hoffmann, J.; Guldimann, A.; James, D. The role of warning behaviors in threat assessment: an exploration and suggested typology. *Behav Sci Law* 2012, *30* (3), 256–279. https://doi.org/10.1002/bsl.999.

[8] Morgado, S.M.A.; Carvalho, M.; Felgueiras, S. Diagnosis model for detection of e-threats against soft-targets. In *Information Systems and Technologies. WorldCIST 2023*; Rocha, A., Adeli, H., Dzemyda, G., Moreira, F., Colla, V., Eds.; Springer: Cham, Switzerland, 2024; Volume 800, pp. 249–262. https://doi.org/10.1007/978-3-031-45645-9_24.

[9] Martins, M. Ciberespaço: uma nova realidade para a segurança internacional. *Nação e Defesa* 2012, *133*, 32–49.

[10] World Economic Forum. *The Global Risks Report 2022*, 17th ed.; World Economic Forum: Geneva, Switzerland, 2022.

[11] Europol. *Internet Organised Crime Threat Assessment (IOCTA) 2021*. Publications Office of the European Union: Luxembourg, 2021. https://doi.org/10.2813/113799.

[12] Moura, R.; Birges, A.; Morgado, S.; Ramalho, N. Police leadership 2.0: A comprehensive systematic review of the literature. *Polic-J Policy Pract* 2022, *17*, 1–11. https://doi.org/10.1093/police/paac068.

[13] Morgado, S.M.A. Inteligência artificial e metamorfose dos paradigmas: Economia na era da transformação. In Proceedings of the Congresso Nacional da Ordem dos Economistas, Lisbon, Portugal, 25-26 October 2023.

[14] European Comission. COM/2017/041 final. *Fourth progress report towards an effective and genuine Security Union*. Publications Office of the EU: Luxembourg, 2017.

© 2025 ITMA. All rights reserved.

[15] Zeman, T. Soft targets: definition and identification. *Acad Appl Resil Publ Manag Sci* 2020, *19*, 109–119. https://doi.org/10.32565/aarms.2020.1.10.

[16] Kalvach, Z. *Basics of soft targets protection–guidelines*. Soft Targets Protection Institute: Prague, Czech Republic, 2016.

[17] Beňová, P.; Hošková-Mayerová, Š.; Navrátil, J. Terrorist attacks on selected soft targets. *J Secur Sustain Issues* 2019, *8*, 453–471.

[18] Morgado, S.M.A.; Neves, L.; Sequeira, P. Policing in sport hall sporting events: a look through several lenses. *Lecturas: Educácion Física Y Deportes* 2023, *28*, 101-118. https://doi.org/10.46642/efd.v28i299.3494.

[19] Schmid, A. Layers of preventive measures for soft target protection against terrorist attacks. In Handbook of terrorism prevention and preparedness; Schmid, A., Ed.; ICCT Press: The Hague, The Netherlands, 2020; pp. 816-839. https://doi.org/10.19165/2020.6.01.

[20] Garcês, B.; Morgado, S.M.A. Estado de Direito versus pandemia: A ação da Polícia de Segurança Pública. *Nação e Defesa* 2022, *165*, 117-132. https://doi.org/10.47906/ND2022.163.06

[21] United Nations. 17 Goals to transform our world. Available online: https://unric.org/en/sdg-1/ (accessed on 9 July 2025).

[22] Morgado, S.; Alves, R. Core capabilities: Body-worn cameras in Portugal *Eur Law Enforc Res Bull* 2019, *18*, 107-122.

[23] Morgado, S.M.A.; Felgueiras, S.; Moura, R. The past, present and the future of technology: preliminary results. In Comemorações dos 40 anos das Ciências Policiais em Portugal; Fernandes, R., Machado, P., Eds; ISCPSI: Lisbon, Portugal, 2024; pp. 389-400.

[24] Morgado, S.M.A.; Nabais, T.; Felgueiras, S. Unveiling the project fAcilitating Public& Private secuRity operAtors to mitigate terrorIsm Scenarios against soft targEts– APPRAISE: the future for preventing and providing security for soft targets. In Comemorações dos 40 anos das Ciências Policiais em Portugal; Fernandes, R., Machado, P., Eds; ISCPSI: Lisbon, Portugal, 2024; pp. 401-412.

[25] Morgado, S.M.A.; San Biaggio, M.; La Matinna, E.; Felgueiras, S. MARPLE: AI-driven threat detection and response for securing soft-targets. In *Information Systems and Technologies. CISTI 2025. Lecture Notes in Networks and Systems* accepted.

[26] Europol. *EU Terrorism situation & Trend report (TE-SAT)*. Publications Office of the European Union: Luxembourg, 2022.

[27] United Nations. *A more secure world: Our shared responsibility*. Report of the High-level Panel on Threats, Challenges and Change. United Nations: New York, NY, USA, 2004.

[28] Creppell, I. The concept of normative threat. *Int Theor* 2011, *3* (3), 450–487. https://doi.org/10.1017/S1752971911000170.

[29] Urinov, B.N. Theoretical aspects of organizational behavior and corporate culture. *Econ Innovative Technol* 2020, 1–8.

[30] Granjo, P. Quando o conceito de «risco» se torna perigoso. *Análise Social* 2006, *XLI* (181), 1167–1179.

[31] Nunes, P. Mundos virtuais, riscos reais: fundamentos para a definição de uma estratégia da informação nacional. *Revista Militar* 2010, *2506*, 1169–1198.

[32] Felgueiras, S.; Morgado, S.M.A. Navigating the Shadows: Content Analysis of Organized Crime Recruitment in the Ozark Series. *Eur Law Enforc Res Bul* accepted.

[33] Beck, U. Risk society towards a new modernity, 2nd ed.; Sage Publications: Newbury Park, CA, USA, 1992.

© 2025 ITMA. All rights reserved.

[34] Eachus, P.; Stedmon, A.; Baillie, L. Hostile intent in public crowded spaces: a field study. *Appl. Ergonomic* 2013, *44* (5), 703–709. https://doi.org/10.1016/j.apergo.2012.05.009.

[35] Castells, M. The rise of the network society, 2nd ed.; Blackwell Publishing Ltd: New Jersey, USA, 2009.

[36] Alotaibi, A.; Hasanat, M.H.A. Racism detection in Twitter using deep learning and text mining techniques for the Arabic language. In Proceedings of the 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH), Riyadh, Saudi Arabia, 3-5 November; IEEE Danvers, United States, 2020; pp. 161–164. https://doi.org/ 10.1109/SMART-TECH49988.2020.00047

[37] Khan, H.; Yu, F.; Sinha, A.; Gokhale, S. A Parsimonious and Practical Approach to Detecting Offensive Speech. In Proceedings of the 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, 19-20 February; IEEE Danvers, United States, 2021; pp. 688–695. https://doi.org/10.1109/ICCCIS51004.2021.9397140.

[38] Mussiraliyeva, S.; Bolatbek, M.; Omarov, B.; Medetbek, Z.; Baispay, G.; Ospanov, R. On detecting online radicalization and extremism using natural language processing. In Proceedings of the 21st International Arab Conference on Information Technology (ACIT), Giza, Egypt, 28-30 November; IEEE Danvers, United States, 2020. https://doi.org/10.1109/ACIT50332.2020.9300086.

[39] Aziz, N.; Maarof, M.; Zainal, A. Hate speech and offensive language detection: a new feature set with filter-embedded combining feature selection. In Proceedings of the 3rd International Cyber Resilience Conference (CRC), Ghent, Belgium, 29-31 January; IEEE Danvers, United States, 2021. https://doi.org/10.1109/CRC50527.2021.9392486

[40] Morgado, S.M.A.; Felgueiras, S. Leveraging technology for public health intervention: A Case study of chatbot AinoAid in addressing domestic violence. In *Information Systems and Technologies. CISTI 2025. Lecture Notes in Networks and Systems* accepted.

[41] Bujlow, T.; Español, C.V.; Pareta, S.J.; Ros, B.P. *Web tracking: mechanisms, implications, and defenses*. ARXIV.ORG Digital Library: 2015.

[42] Weert, A.; Eijkman, Q. Early detection of extremism? The local security professional on assessment of potential threats pose by youth. *Crime Law Soc Chang* 2019, *73*, 491–507. https://doi.org/10.1007/s10611-019-09877-y.

[43] Morgado, S.M.A.; Ferraz, R. Análise de conteúdo e pesquisa em ciências policiais: Contextualização em ambiente virtual, facebook, e o planeamento de grandes eventos. In *Investigação Qualitativa em Ciências Sociais*; Costa, A.P., Tuzzo, S., Ruano, L., Silva, C.T., Souza, F.N., Souza, D.N., Eds.; CIAQ: Lisboa, Portugal, 2016; Volume 3, pp. 600–608.

[44] Morgado, S.M.A.; Ferraz, R. Social media: facebook e a gestão policial no planeamento de grandes eventos. *Int J Mark Commun* 2016, *Special Number 1*, 27–47.

[45] Morgado, S. Going Global: Health organizations and networking – information society and social media. In Proceedings in Scientific Conference 2013, Žilina, Slovakia; Mokryš, M., Badura, S., Lieskovský, A. Eds; Thomson: Slovakia, 2013; pp. 47–51.

[46] Morgado, S.; Alfaro, R. Technology embracement in objective driven police: UAV's in public security police in Portugal. In International Conference on Risks, Security and Citizens: Proceedings/Atas, Setúbal, Portugal, 30-31 March; Teixeira, N.S., Oliveira, C.S., Lopes, M., Sardinha, B., Santos, A., Macedo, M., Eds.; Município de Setúbal: Setúbal, Portugal, 2017; pp. 298–305.

© 2025 ITMA. All rights reserved.

[47] Mendes, S.; Morgado, S. Intelligence services intervention: Constraints in portuguese democratic state. In *International Conference on Risks, Security and Citizens: Proceedings/Atas*, Setúbal, Portugal, 30-31 March; Teixeira, N.S., Oliveira, C.S., Lopes, M., Sardinha, B., Santos, A., Macedo, M., Eds.; Município de Setúbal: Setúbal, Portugal, 2017; pp. 285–297.

[48] Morgado, S.M.A.; Xavier, C.; Pereira, P. Prevention and road safety campaigns through emotion in Portugal: a comprehensive empirical analysis. In *Marketing and Smart Technologies. ICMarkTech 2023. Smart Innovation, Systems and Technologies*; Reis, J.L., Zelený, J., Gavurová, B., dos Santos, J.P.M., Eds.; Springer: Cham, Switzerland, 2025; Volume 393, pp. 139-155. https://doi.org/10.1007/978-981-97-3698-0_10.

[49] Campbell, T.A. *Artificial intelligence: an overview of state initiatives*. Future Grasp, LLC: Evergreen, CO, USA, 2019.

[50] Risi, F.T.; Pera, A. *Artificial Intelligence in the field of criminal law*. In Special collection: Artificial Intelligence; UNICRI: Torino, Italy, 2020; pp. 6–17.

[51] Morgado, S.M.A.; Felgueiras, S. Technological Policing: Big Data versus Real Data. *Politeia – Revista Portuguesa de Ciências Policiais* 2022, *XIX*, 139–151. https://doi.org/10.57776/hkcb-br21.

[52] Bernal, P. Data gathering, surveillance and human rights: recasting the debate. *J Cyber Policy* 2016, *1* (2), 243–264. https://doi.org/10.1080/23738871.2016.1228990

[53] Bridges, L.E. Digital failure: Unbecoming the "good" data subject through entropic, fugitive, and queer data. *Big Data Soc* 2021, *8* (1), 2053951720977882. https://doi.org/10.1177/2053951720977882

[54] Sanders, C.B.; Sheptycki, J. Policing, crime and 'big data'; towards a critique of the moral economy of stochastic governance. *Crime Law Soc Chang* 2017, *68*, 1–15. https://doi.org/10.1007/s10611-016-9678-7

[55] UNICRI. *Strategic programme framework*. UNICRI: Torino, Italy, 2020.

[56] Risse, M. Human rights and artificial intelligence: an urgently needed agenda. *Hum Rights Q* 2019, *41* (1), 1–16. https://doi.org/10.1353/hrq.2019.0000

[57] Council of Europe. *CETS 005 - Convention for the protection of human rights and fundamental freedoms*; Publications Office: Brussels, Belgium, 2019.

[58] Wakefield, A. The public surveillance functions of private security. *Surveill Soc* 2002, 2 (4), 529-545. https://doi.org/10.24908/ss.v2i4.3362

[59] Benson, B.L. Crime control through private enterprise. *Independent Rev* 1998, *2* (3), 341–371.

[60] European Parliament, Council of the European Union. *EU Directive 95/46/EC - on the protection of individuals with regard to the processing of personal data and on the free movement of such data*; Publications Office: Brussels, Belgium, 1995.

[61] Custers, B.; Uršič, H. Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection. *Int Data Privacy Law* 2016, *6* (1), 4–15. https://doi.org/10.1093/idpl/ipv028

[62] Risse, M. Human rights and artificial intelligence: an urgently needed agenda. *Hum Rights Q* 2019, *41* (1), 1–16. https://doi.org/10.1353/hrq.2019.0000

[63] Council of Europe. *Council Framework Decision 2008/977/JHA - On the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*; Publications Office: Brussels, Belgium, 2008.

© 2025 ITMA. All rights reserved.

[64] European Commission. Directorate-General for Communications Networks, Content and Technology. *Ethics guidelines for trustworthy AI*; Publications Office: Brussels, Belgium, 2019. https://doi.org/10.2759/346720

[65] European Commission. Directorate-General for Communications Networks, Content and Technology. *Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment*; Publications Office: Brussels, Belgium, 2020.

[66] European Commission. *Ethics by design and ethics of use approaches for artificial intelligence*; European Commission: Brussels, Belgium, 2021.

[67] Land, M.K.; Aronson, J.D. Human rights and technology: new challenges for justice and accountability. *Ann Rev Law Soc Sci* 2020, *16*, 223–240. http://dx.doi.org/10.2139/ssrn.3690635

[68] Lei, Y.; Yang, B.; Jiang, X.; Jia, F.; Li, N.; Nandi, A.K. Applications of machine learning to machine fault diagnosis: a review and roadmap. *Mech Syst Signal Process* 2020, *138*, 106587. https://doi.org/10.1016/j.ymssp.2019.106587

[69] Pfisterer, F.; van Rijn, J.N.; Probst, P.; Müller, A.C.; Bischl, B. Learning multiple defaults for machine learning algorithms. In Proceedings of the Genetic and Evolutionary Computation Conference Companion, Kyoto, Japan, 13-17 July, Association for Computing Machinery: New York, United States, 2021; pp. 241–242.

[70] Morgado, S.M.A.; Felgueiras, S. Big Data in Policing: Profiling, patterns, and out of the box thinking. In *Trends and Applications in Information Systems and Technologies. WorldCIST 2021*; Rocha, Á., Adeli, H., Dzemyda, G., Moreira, F., Ramalho Correia, A.M., Eds.; Springer: Cham, Switzerland, 2021; Volume 1365, pp. 217–226. https://doi.org/10.1007/978-3-030-72657-7_21

[71] Khanzode, K.C.A.; Sarode, R.D. Advantages and disadvantages of artificial intelligence and machine learning: a literature review. *Int J Libr Inf Sci* 2020, *9* (1), 30–36.

[72] Ray, S. A quick review of machine learning algorithms. In Proceedings of the 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), Faridabad, India, 14-16 February; IEEE: Danvers, United States, 2019; pp. 35–39. https://doi.org/10.1109/COMITCon.2019.8862451

[73] Boin, A., Comfort, L.K., Demchak, C.C. The rise of resilience. In *Designing Resilience Preparing Extreme Events*; Confort, L. K., Boin, A., Eds.; University of Pittsburgh Press: Pittsburgh, USA, 2010; pp. 1–12.

[74] Beridze, I. *Foreword*. Special collection: Artificial Intelligence. UNICRI, Torino, Italy, 2020.

[75] Felgueiras, S., Pais, L.G., Morgado, S.M.A. Interoperability: Diagnosing a novel assess model. *Eur Law Enforc Res Bull* 2018, (4 SEC), 255–260.

© 2025 ITMA. All rights reserved.