JCBRN Defence COE
per virtutem ad securitatem

HIGH-IMPACT, LOW-PROBABILITY

NATO-EUROPOL COOPERATION IN COUNTERING THE CBRN TERRORIST THREAT TO EUROPE

Mathias KATSUYA

Supervised by Tomáš MICHALČÍK

2024

Disclaimer

The publication reflects the author‘s positions, views, findings, interpretations and conclusions as an independent academic opinion. It is not a North Atlantic Treaty Organization (NATO) endorsed or approved document and does not reflect neither NATO‘s nor individual government‘s policies or positions nor does it reflect the policies or positions of the JCBRN Defence COE or its Sponsoring Nations and Contributing Partner. Although the JCBRN Defence COE has invested the utmost care in its preparation, the JCBRN Defence COE does not accept any liability for the accuracy and completeness of any information, instruction and/or advice provided, as well as for misprints. No claims can be made against the JCBRN Defence COE concerning potential consequences from the reliance on information or conclusions contained herein.

JCBRN Defence COE (2024): High-Impact, Low-Probability: NATO-EUROPOL Cooperation in countering the CBRN Terrorist Threat to Europe.

Cover Image © Globalofficeatom | Dreamstime.com | Used in accordance with the Dreamstime.com licensed usage terms

JOINT CHEMICAL, BIOLOGICAL, RADIOLOGICAL AND NUCLEAR DEFENCE CENTRE OF EXCELLENCE

Víta Nejedlého
682 01, Vyškov
Czech Republic

Phone: +420 973 452 777
IVSN: 925 4200 452 777
E-mail: postbox@jcbrncoe.org

www.jcbrncoe.org

www.twitter.com/jcbrncoe
linkedin.com/company/jcbrndefencecoe

Summary

Terrorist incidents involving the release of CBRN substances have long constituted a nightmare scenario for the Euro-Atlantic community. Though CBRN terrorism today largely centres on lone jihadist and right-wing extremist actors employing rudimentary chemical or biological agents, contemporary global challenges like climate change and escalating strategic competition following Russia's 2022 invasion of Ukraine have broadened the CBRN threat picture to encompass new adversaries, such as radical environmentalists and hostile states. When combined with technological advancements, including the democratisation of scientific knowledge through AI-based large language models and the proliferation of unmanned vehicles, the opportunities and incentives for the use of CBRN terrorism as a strategic tool for political ends have significantly increased.

CBRN counterterrorism in the European context is, fundamentally, a law enforcement responsibility; nevertheless, the sheer scale of resources required to respond to these incidents has traditionally necessitated the deployment of military assets in support of civil authorities. At the same time, emerging technologies and hostile actors have rendered CBRN counterterrorism both an increasingly cross-sectoral and cross-border effort. As respective focal points for military and law enforcement cooperation in Europe, NATO and Europol are uniquely positioned to enable this degree of multi-national, whole-of-government engagement which defines the CBRN problem-set.

This report draws on secondary-source research and insights provided by JCBRN Defence COE personnel as well as Europol's CBRN-E Team Leader. An initial threat assessment is followed by a review of Europol's CBRN capabilities, centring on the role of its European Counter-Terrorism Centre and in-house CBRN-E Team as key nodes in law enforcement information-sharing, capacity-building, and operational coordination. Having identified key doctrinal and capability overlaps with NATO in addition to a stated commitment by Europol's CBRN-E Team to enhance its civil-military relations, the report outlines a three-pillar approach to deepening connections between NATO and Europol: short-term measures to foster staff-level contacts in both organisations, a formalised relationship between Europol's CBRN-E Team and NATO's JCBRN Defence COE, and deeper institutional linkages to effectively confront current and emerging CBRN threats.

Contents

1. CBRN Terrorism and the European Context

The genesis of contemporary efforts to counter violent non-state actor use of chemical, biological, radiological, and nuclear (CBRN) weapons is inextricably tied to perceived shifts in the broader terrorist threat. Historical incidents such as the Palestinian Black September Organisation's hostage-taking at the 1972 Munich Olympic Games, which resulted in the deaths of 11 Israeli athletes, cemented a particular conceptualisation of the terrorist actor; in the words of Brian Michael Jenkins, "terrorists want a lot of people watching, not a lot of people dead" (Jenkins 1985, 22). In effect, the use of violence by terrorist organisations was regarded as clearly instrumental, directed towards the achievement of articulable political objectives and tempered by self-imposed limitations.

This understanding, however, would come under increasing assault throughout the 1990s, a period which witnessed a decline in international terrorist attacks but, conversely, a troubling rise in lethality. A thirteen-year series of mass casualty incidents, beginning with the 1988 bombing of Pan Am 103 and culminating in the 9/11 attacks, gave rise to the concept of "new terrorism", driven by religious or political goals so abstract they were overshadowed by increasingly shocking and indiscriminate destruction (Bolanos 2014, 31). Violence, in effect, was no longer a means to an articulable political end but an end in itself. As one former US Director of Central Intelligence remarked, "today's terrorists don't want a seat at the table, they want to destroy the table and everyone sitting at it" (Morgan 2004, 30-31). To the 'new' terrorist, CBRN weapons represented an attractive means of achieving this end of pure violence.

It was precisely within this period that the defining act of CBRN terrorism occurred. On 20 March 1995, members of the Japanese cult, Aum Shinrikyo, boarded five Tokyo subway trains and pierced packets of sarin nerve agent with their umbrellas, killing fourteen people and injuring over one thousand (Parachini 2005, 23-24). While the impacts of the Aum's actions were limited, in large part due to weak sarin and a flawed delivery system, the Tokyo attacks confirmed the worst fears of the new terrorism thesis' proponents and saw CBRN counterterrorism elevated to a national security priority. It is important to note, however, that since the Aum, visions of large-scale CBRN attacks on civilian targets have yet to materialize. The deadliest means employed by terrorist organizations are, instead, decidedly traditional – "bombs, conventional explosives, and most famously box cutters" (Spencer 2006, 19).

While CBRN terrorism, thus, remains a high-impact low-probability event, emerging technologies have only increased the lethality and accessibility of these weapons. Advances in additive manufacturing and unmanned vehicles now allow terrorist organisations to develop sophisticated CBRN systems, including the use of aerial drones as dispersal platforms for chemical munitions or biological and radiological substances (Cetina and Jozić 2022, 136)[1]. At the same time, the proliferation of artificial intelligence software has democratised the technical expertise required to perpetrate CBRN attacks. A 2023 study, for instance, saw American university students exploit large language models to plan the weaponisation of a pathogen and source the necessary biological materials in less than one hour (Cordova et al. 2023, 2-3). Understanding the precise scale of this threat to European states, however, necessitates a thorough evaluation of terrorist CBRN capabilities.

1.1. Evaluating the Threat: Jihadist Terrorism

Jihadist violence has traditionally been regarded as Europe's most severe terrorist threat, both in lethality and socio-political ramifications. It is important to note that it was the jihadist attack against the United States on 11 September 2001 that resulted in the first, and only, invocation of the North Atlantic Treaty Organisation's (NATO) collective defence provisions (Grady 2002, 169). The term "jihadism", itself, refers to a violent sub-current of Sunni Salafism, which seeks to forcibly establish an Islamic state

[1] For a more detailed assessment of the employment of unmanned systems and implications of technological development, please see the JCBRN Defence COE Study, "Role of Uncrewed Vehicles (UxVs) in CBRN Defence."

governed by sharia law (Europol 2023b, 23) Historically, al-Qaeda (AQ) and the Islamic State in Iraq and Syria (ISIS) constitute the primary drivers of CBRN jihadist terrorism.

AQ and ISIS' CBRN programmes vary significantly in scale and sophistication. While AQ pursued a full spectrum of capabilities ranging from nuclear devices and anthrax to crude poisons, ISIS focused its efforts on simple chemical weapons such as sulphur mustard and battlefield delivery through improvised explosive devices and mortars (Ananthan and Dass 2021, 559) Both groups' capacities, however, to mount CBRN attacks beyond their immediate geographic regions are severely limited. Relentless international military efforts, including the ongoing US-led Operation Inherent Resolve and NATO Mission-Iraq, have degraded jihadist capabilities and hindered organisational resurgence, while the corrosive and volatile nature of easily manufactured CBRN substances largely precludes long-distance transportation (Hummel 2016, 20). Jihadist attacks in Europe would, thus, likely be staged internally, relying on rudimentary chemical or biological agents that could be produced and employed in rapid succession.

Central to the continued viability of this threat is the rise of the lone actor model. Rather than elaborate, externally-directed operations, groups such as ISIS now seek to inspire individuals or autonomous cells to operate on their behalf domestically, with jihadist propaganda proposing small-scale CBRN attacks with legally acquired toxins and industrial chemicals (Europol 2018, 14). The effects of this tactical shift are already visible in the domain of CBRN terrorism. 2018, for instance, saw three lone actor CBRN plots by jihadists in Europe, including separate attempts in France and Germany to produce ricin - a biological toxin extracted from castor beans through a basic chemical process (Fade 2018, 3). While the current jihadist CBRN threat is, therefore, limited in its sophistication, lone actors have demonstrated a willingness to leverage emerging technologies to their advantage. Most recently, a 2023 case in the United Kingdom involved an engineering student producing a 3-D printed unmanned aerial vehicle as a chemical weapon delivery system for the Islamic State (Counter Terrorism Policing, "Man found guilty"). Regardless of their ultimate lethality, the corrosive psychological effect of such unconventional attacks results in a potential for major disruption, even if rudimentary CBRN weapons fail to physically harm large numbers of people.

1.2. Evaluating the Threat: Right-Wing Terrorism

Violent right-wing extremism represents a key emerging threat for European states. Here, the term "right-wing extremism" encompasses a broad ideological umbrella, with core themes including "exclusionary nationalism, racism, xenophobia, and/or related intolerance" and an associated commitment to violently reject democratic values (Europol 2023b, 43). As with contemporary trends in jihadist movements, far-right CBRN terrorism constitutes an overwhelmingly lone-actor phenomenon. Perpetrators are most "middle-aged and comparatively well-educated" males, with violence directed towards "indiscriminate" targets (Koehler and Popella 2018, 1685). This lack of centralized leadership and support has not inhibited the development of CBRN capabilities among right-wing terrorist extremists.

Far-right actors have continually pursued the acquisition, weaponization, and employment of CBRN agents. While such efforts in the United States centre overwhelmingly on simple toxins and chemicals such as ricin and cyanide, right-wing extremists have not hesitated to exploit sophisticated technical systems in their plots; one 2013 attempt, for instance, involved the construction of a radiation emitting device, described as "Hiroshima on a light switch" by white supremacists (Fleer 2020, 233). This degree of ambition, however, is not visible among the European far-right. Since 2000, right-wing extremists have been involved in four CBRN plots, all involving chemical weapons, with the most severe incident being the release of mace during the June 2008 Queer Parade in the Czech city of Brno, resulting in four injuries (Sin and Binder 2022).

While contemporary far-right CBRN terrorism in Europe is restricted in scale and complexity, the threat posed remains in a state of constant evolution. In addition to elevating the lethality of attacks, technological advancement has fuelled an unprecedented exchange of previously restricted tactical and technical expertise, a central facet of the growing "internationalisation" of far-right extremism (Pauwels 2021, 6). And with this continued movement of knowledge and ideas across physical and digital

boundaries, the potential for a significant escalation in the CBRN threat posed by violent right-wing groups in Europe cannot not be dismissed.

1.3. Evaluating the Threat: Ethno-Nationalist Terrorism

Ethno-nationalist terrorism represents a consistent, albeit declining, threat to European security. Here, "ethno-nationalist" refers to organisations employing violence in pursuit of political objectives rooted in "nationalism, ethnicity, and/or religion" as well as separatist movements seeking to establish independent states (Europol 2023b, 66). While scholars have traditionally regarded the willingness of these movements to conduct CBRN attacks as limited by a need to retain constituent support and avoid retaliatory attacks, ethno-nationalist groups have consistently employed CBRN agents against military and civilian targets (Meulenbelt and Niuewenhuizen 2015, 841).

The most prominent examples of ethno-nationalist CBRN terrorism have occurred beyond the territories of NATO and the European Union. In fact, the first deployment of a chemical agent by a violent non-state actor occurred in 1990, when members of the Liberation Tigers of Tamil Eelam, which sought the creation of an independent Tamil state from Sri Lanka, released chlorine gas on a Sri Lankan military encampment (Hoffman 2009, 470-471). Between 1994 and 2002, Chechen separatists perpetrated four fatal attacks with chemical agents and toxins, in addition to repeatedly threatening to detonate improvised explosive devices containing radioactive material (Sin and Binder 2022). It is important to note, however, that these actions occurred amidst high-intensity insurgent conflicts, a reality simply not reflected in Europe today.

Instances of CBRN terrorism by contemporary European ethno-nationalist groups are, instead, limited. Since 2000, eight instances of attempted or threatened use of CBRN substances have occurred, six involving chemical and biological agents in addition to two plots involving radiological and nuclear materials; over the same period, two successful acts of CBRN terrorism were perpetrated, with only one, the bombing of the Feliz Bailondo chemical factory by Basque separatists, producing any injuries (Ibid). With the continued decline in ethno-nationalist and separatist violence across Europe, the potential for additional CBRN attacks remains remote.

1.4. Evaluating the Threat: Single-Issue Terrorism

Single-issue terrorism encompasses the greatest diversity of drivers behind violent mobilization and refers to groups employing "criminal means" to alter policies or practices in specific domains such as environmental protection or animal rights (Europol 2022b, 91). Historically, single-issue movements have overwhelmingly adopted non-violent tactics such as peaceful protests and blockades. Since 1992, five CBRN attacks by such groups have occurred in Europe, all involving dual-use chemicals delivered through aerosol canisters or contaminated food and drink and resulting in only one fatality (Sin and Binder 2022).

Despite this limited precedent, contemporary developments risk pushing single-issue movements increasingly towards violence. Climate change, for instance, has the potential to "energise" radical environmentalists and provide "increasingly strong justifications" for terrorism (Bleek and Kallenborn 2018, 359). Green anarchist organisations, seeking the complete destruction of societal and industrial systems seen as enabling continued degradation, have attempted catastrophic CBRN attacks, such as a 1972 attempt to poison Chicago's water supply with typhoid bacteria (Carus 2000, 56). With atomic power also reemerging as a vital sustainable energy option, the confluence of environmentalist and anti-nuclear groups directing attacks against nuclear facilities cannot be dismissed. Though most previous attacks occurred during the construction phases, the possibility exists that fringe elements may view actions resulting in radiation leaks as a "prime option" for highlighting the continued dangers of nuclear power (Ferguson et al. 2005, 25). Single-issue CBRN terrorism, thus, constitutes an evolving threat with the potential for significant escalation amidst a worsening climate crisis.

1.5. A Note on State-Based Threats

The notion of 'state terrorism' is, itself, highly contentious. This report employs NATO's definition of terrorism as a conceptual starting point and defines 'state terrorism' as a tactic, centring on the "unlawful use or threatened use" of violence to instil "fear and terror" as a means of achieving broader political

objectives (NATO "Terrorism"). To this end, state actors have not hesitated to employ CBRN weapons in campaigns of assassination and political intimidation. From North Korea's assassination of Kim Jong Nam in Malaysia with VX nerve agent to the Syrian government's employment of chemical weapons against civilians, the global normative and regulatory architecture restricting CBRN employment has come under increasing assault (Tu 2020, 52; Human Rights Watch "Death by Chemicals").

For NATO and EU states, however, it is the Russian Federation that presents the most direct threat in the domain of state CBRN terrorism. Russian special services perpetrated the "first provable act of radiological terror", with the 2006 murder of Alexander Litvinenko with polonium-210 and have been linked to the continued use of chemical weapons since, including the poisoning of defectors and political opponents employing Novichok nerve agent and organochlorine compounds (Acton et al. 2007, 151; Weiss "Blood Simple"). Such attacks are notable for both their visibility and complexity, with the involvement of a state's intelligence and security apparatus frequently entailing the use of sophisticated CBRN agents.

It is also possible to envision instances of state CBRN terrorism beyond assassination. In 2021, Czech authorities revealed Russian military involvement in a series of explosions at an arms depot in Vrbetice, resulting in two fatalities (Bellingcat "Senior Gru Leader"). Though the operation targeted stored conventional munitions, adversarial action against CBRN infrastructure cannot be ruled out. Russia's 2022 capture of Ukraine's Zaporizhzhia Nuclear Power Plant, for instance, sparked concerns over its potential use as a "giant dirty bomb", with a deliberate release of radiation serving to tie-up Ukrainian military resources and sow fear within the civilian populace (Dolzikova "Degradation Everywhere"). Perhaps the most pressing security consequence stemming from the Russian invasion of Ukraine, however, is the increased potential for CBRN proliferation due to criminal or military activity. The theft or diversion of small-arms and light weapons to illicit buyers in Western Europe has already been identified as an emerging security concern, with the loss of regulatory control over CBRN and explosive material similarly constituting a potential acquisition source for violent non-state actors (GI-TOC 2024, 57). As strategic competition between NATO and the Russian Federation intensifies, it is likely that CBRN terrorist threats stemming from direct, or indirect, state action will pose a continued challenge to the rules-based international order.

Takeaway: The CBRN terrorist threat facing Europe is in a state of evolution. While jihadist and right-wing lone actors remain the predominant security concern, the traditional notion of rudimentary attacks with crude chemical or biological agents must be reconciled with technological advancement in domains such as unmanned systems and artificial intelligence that render CBRN capabilities increasingly accessible and sophisticated. At the same time, CBRN attacks by single-issue environmentalist groups as well as malign states represent a key emerging challenge for NATO and the EU, with developments like continued environmental degradation and strategic competition constituting drivers for escalation in the scale and impacts of potential incidents. Regardless of their ultimate lethality, however, it is important to note that perhaps the most significant effect of CBRN weapons is their disproportionate psychological impact, yielding long-term socioeconomic and political ramifications at the strategic level.

2. CBRN Counterterrorism and the Euro-Atlantic Community

Terrorism in Europe has long been presented as a fundamentally criminal, rather than military, threat. In the words of European Counter-Terrorism Coordinator Gilles de Kerchove, terrorists must be "investigated, prosecuted, and convicted wherever possible according to the normal rules of criminal law" (Devoic 2012, 114-115). Civilian law enforcement, thus, holds primacy in the prevention of and response to terrorism on the European continent. Exceptions to this do exist, and certain incident types

necessitate the involvement of the armed forces due to the degree of training, equipment, and resources required. Notable among these is CBRN counterterrorism, with the North Atlantic Treaty Organisation (NATO) affirming that "military units and activities have often proven to be a critical component for successful [CBRN] response operations" (NATO 2014, 6). It is, nevertheless, vital to note that the armed forces remain an enabling asset, functioning in support, as opposed to in lieu, of civil authorities.

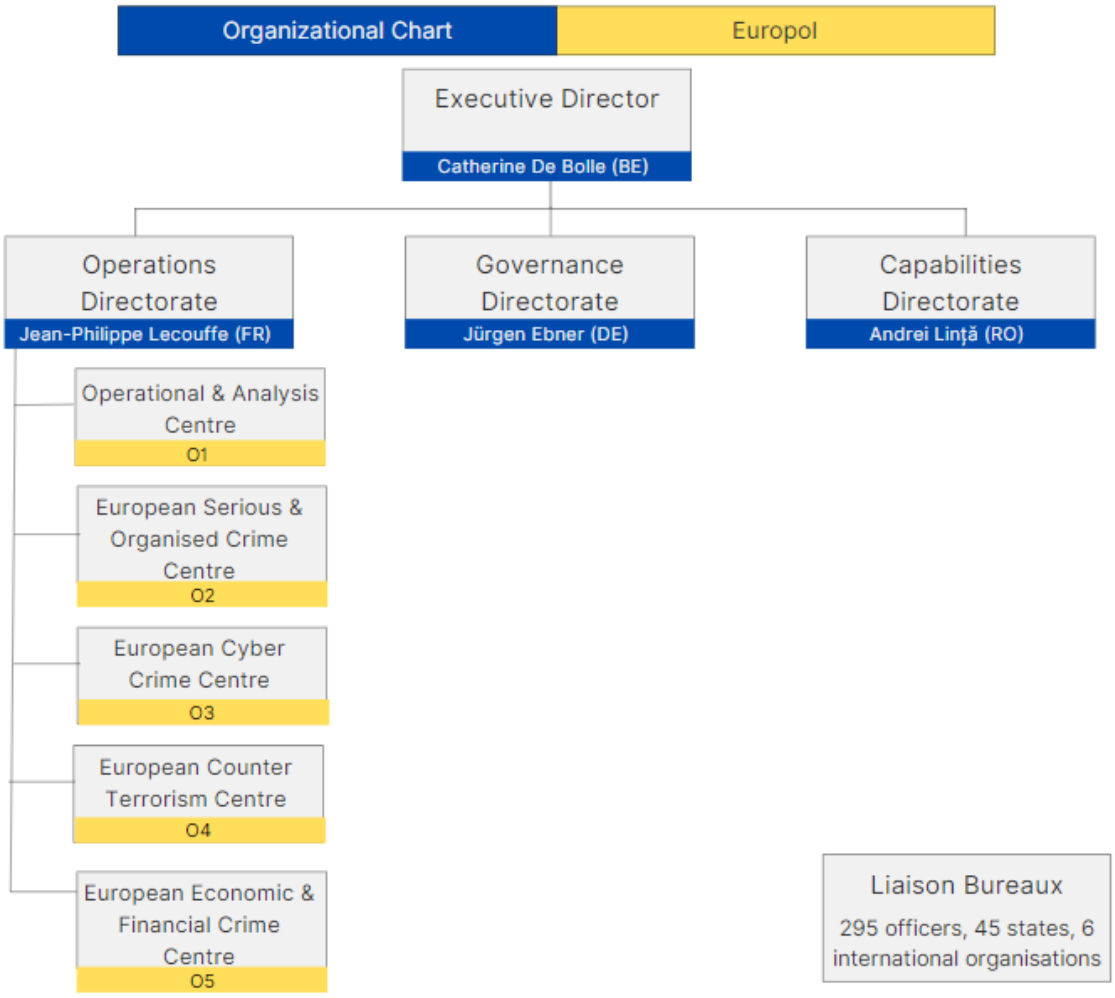
While the current CBRN terrorist challenge has largely centred on rudimentary chemical or biological attacks by jihadist or violent right-wing groups, the EU recognises that emerging technologies and adversaries, detailed in Section I of this report, render CBRN terrorism an increasingly "cross-border and transnational threat" (DG HOME 2017, 7). Successful prevention or response will, therefore, push civilian law enforcement agencies to engage across borders with both one another and supporting military assets. This report, in turn, investigates the potential for a deepened relationship between two pillars of Europe's security cooperation architecture in combating violent non-state actor use of CBRN weapons: NATO and the European Union Agency for Law Enforcement Cooperation (Europol). Before this theme can be fully explored, however, it is essential to first understand precisely what Europol and its role in CBRN counterterrorism is.

2.1. Europol 101

Europol is one of the EU's most important law enforcement actors, tasked with supporting Member States in their fight against serious organised crime, terrorism, and cyber offences. A full EU agency since 2010, Europol is accountable to the Council of Ministers for Justice and Home Affairs, comprising relevant ministers from each EU Member State (Europol "About Europol"). Despite initial visions for a "European FBI" capable of unilaterally confronting transnational criminal activity, Europol officers possess no powers of arrest and cannot launch independent investigations (König and Trauner 2021, 181). The agency's mission, instead, centres on enabling the activities of national law enforcement authorities within EU Member States.

Central to fulfilling this task is an array of unique platforms and capabilities. Among others, Europol manages the Secure Information Exchange Network Application to quickly respond to requests for strategic and operational data, conducts analysis projects that feed into Member State criminal intelligence cycles, and delivers real-time coordination and support to cross-border police operations (Europol 2023d, 9-12). Much of this responsibility is concentrated within the Operations Directorate. In addition to a 24/7 Operational and Analysis Centre, the directorate consists of four thematic departments providing assistance to Member State agencies in each of Europol's key crime areas (Europol "Operational and Analysis Centre"). Perhaps most significantly, the agency possesses an ever-expanding array of connections with Member State law enforcement authorities and other multinational entities. Europol National Units exist within every EU police force as dedicated points-of-contact for information sharing, while Europol's Liaison Bureaux count 295 officers from EU/non-EU states as well as international organisations such as Interpol or European military forces (Europol "Statistics & Data).

This sheer degree of connectivity renders Europol an increasingly prominent conduit for criminal intelligence and information sharing between EU national authorities as well as external partners. When combined with its robust analytical and operational support capacities, Europol finds itself uniquely positioned to enhance collective situational awareness and coordinate the cross-border law enforcement response that a CBRN terrorist incident will undoubtedly require.



(Europol "About Europol"; Europol "Statistics & Data")

2.2. Europol as a CBRN Counterterrorism Actor

The fight against violent extremism constituted a particularly contentious facet of Europol's mission, with the organisation possessing limited counterterrorism as well as CBRN dDefence resources and responsibilities upon its founding. In fact, the very inclusion of terrorism within Europol's competencies was largely driven by Spain, itself confronting continued violence from the Basque separatist movement ETA, and only entered into force in 1999 after a negotiated agreement with a reticent France (Kaunert 2010, 654). Much like NATO, which previously identified terrorism as merely another "[risk] of a wider nature", the events of 11th September 2001 marked a paradigm shift in Europol's CBRN defence and counterterrorism competencies (Bernasconi 2011, 2). The Extraordinary European Council meeting held ten days after the attack resulted in the formation of a 24-hour Counter Terrorist Task Force within Europol, comprising internal experts as well as national police and intelligence liaison officers to provide real-time operational and strategic analysis (Bures 2008, 502). A December 2002 European Council Decision built upon this and stipulated that Member States were obligated to communicate information to Europol concerning, among others, the potential for terrorist acquisition and employment of CBRN weapons (European Commission 2002, 68).

Despite these sweeping institutional changes, Europol's capacity to strengthen and support Member State efforts in the domain of CBRN counterterrorism remained limited. The Counter-Terrorist Task Force faced criticism from EU and external officials for its shortfalls in handling real-time data, and its overall operational scope was highly restricted (Bensahel 2003, 40). Nevertheless, Europol established an array of functionally specialised programmes, which gradually broadened the agency's counterterrorism and

CBRN defence responsibilities. Its "Counter Proliferation Programme" assisted Member States in addressing the illicit trafficking of CBRN materials and explosives, while the "Preparedness Programme" centred on crisis management and the formation of multi-lateral investigative teams to respond to terrorist incidents; finally, a "Training and Education Programme" was established to provide instruction to Member State personnel in fields such as Explosive Ordnance Disposal (EOD) and CBRN response (Deflem 2006, 346). While still hindered by the reluctance of Member States to engage in robust information-sharing, Europol's degree of involvement in countering terrorism and CBRN threats in the 2000s expanded significantly from the organisation's founding one decade earlier. But it would be events closer to home that would provide the second inflection point in the agency's path to becoming an increasingly prominent CBRN counterterrorism actor.

2015 constituted a defining year in the development of Europol's counterterrorism policies and capabilities. The Islamic State's coordinated attacks in Paris on 13 November, the deadliest terrorist incident in the EU since the 2004 Madrid train bombings, pushed intelligence sharing with Europol to unprecedented heights, as France moved quickly to provide the agency with sensitive data on foreign fighters (Bossong 2018, 3). Other EU Member States soon joined, and the reticence that once hampered Europol's analytical and operational efforts in counterterrorism was pushed aside. Amidst this increased institutional engagement by national police authorities, the European Counter Terrorism Centre was established within Europol as the nucleus for combined law enforcement efforts against violent extremism at the EU level (Europol "European Counter Terrorism Centre"). It is this body that is, today, at the heart of Europol's current role as a CBRN counterterrorism actor.

2.2.1. The European Counter Terrorism Centre CBRN-E Team

The European Counter Terrorism Centre (ECTC or O4) is one of four thematic departments within Europol's Operations Directorate. Founded in January 2016, ECTC was designed as the key EU-level body for law enforcement information-sharing to better analyse and assess the terror threat facing Member States as well as assist in the development of operational plans (European Commission 2016, 10). Perhaps most significantly, ECTC retains primacy for Europol's response to terrorist acquisition, proliferation, or use of CBRN and explosive (CBRN-E) weapons. This is achieved through a dedicated CBRN-E Team, a five-member unit of EOD and CBRN specialists that serves as a "central knowledge hub" for ECTC, other Europol departments, and Member State law enforcement agencies (DG HOME 2017, 13).

ECTC's CBRN-E Team works to maintain situational awareness of current and emerging CBRN and explosive threats. To this end, the team works closely with Europol Analysis Projects (AP) such as AP Weapons and Explosives under the Serious & Organised Crime Centre, focusing on the possession or trafficking of small arms and CBRN-E materials, or ECTC's AP Check-the-Web, conducting open-source monitoring to prevent terrorist abuse of online platforms (Europol "Europol Analysis Projects"). Its status as a technical unit supporting the Operations Directorate's departments allow the team to draw on Europol's varying analytical streams to provide a wholistic understanding of CBRN-E challenges. This, in turn, feeds into technical and threat assessments disseminated to EU Member States (Simões, 2024). In 2019, for instance, the CBRN-E Team provided guidance to national investigations targeting the illicit online sales of chemicals as well as industrial precursors used in the creation of improvised explosive devices (Europol 2020b, 30). This support to Member States, however, extends beyond strategic analysis and encompasses direct operational assistance.

In addition to headquarters-based assessments, the CBRN-E Team possesses the capability to deploy and provide on-the-spot support at the request of a Member State. 2019, notably, saw Europol participate in a tri-national investigation - comprising Austria, Moldova, and Slovakia – into the smuggling of nuclear material to an armed group, with a CBRN-E Team member accompanying the final arrest operation in Vienna (Europol "Crime Group Suspected"). It is important to note that the CBRN-E Team's role in such instances centres not on its technical expertise but on its direct reach to Europol's information platforms. Member States can access sensitive information on common platforms to a limited extent, with the creation of closed-user groups within Europol's SIENA software allowing for direct communication of operational and personal details between states (Bossong 2018, 4). Europol, however, also retains internal databases containing sensitive intelligence Member States elect to provide only to the organisation; the deployed CBRN-E Team member, in turn, provides a "mobile office"

capability, facilitating the exchange of this sensitive information and allowing national authorities to situate individual CBRN threats within broader criminal or terrorist trends observed in other states (Simões, 2024). Ultimately, the 2019 investigation highlights not only the increasingly transnational nature of CBRN threats but also the role of ECTC and its CBRN-E Team as key nodes in the intelligence-sharing vital to counterterrorism successes.

Beyond these analytical and operational responsibilities, ECTC's CBRN-E Team plays a central role in both capacity-building and strengthening linkages between Member State CBRN counterterrorism practitioners. Alongside the EU Agency for Law Enforcement Training (CEPOL), the team identifies training gaps and organises programmes leveraging existing pools of resources and expertise within Member States, with one 2022 course involving over 70 EOD and CBRN specialists alone (Europol 2023a, 30). These training events are complimented by an array of online systems, allowing for the continuous flow of insights and lessons-learned among CBRN counterterrorism practitioners. The CBRN-E Team, for instance, manages the European Bomb Data System as well as the Europol Platform for Experts/European EOD Network, which include CBRN-E incident databases as well as discussion forums for exchanging best practices (Simões, 2024). Membership in these platforms is not restricted to law enforcement personnel and can be granted to competent authorities in the domain of CBRN response and counterterrorism, including military units (Europol 2011, 2). When combined with its capacities for strategic and operational support, ECTC and its CBRN-E Team are uniquely positioned to serve as an organisational focal point for CBRN counterterrorism cooperation between EU Member States, institutions, and key external partners.

2.2.2. The ATLAS Network

ECTC also retains direct institutional links with the ATLAS Network, another vital law enforcement actor in the domain of CBRN counterterrorism. Formalised in the aftermath of the 11th September attacks, ATLAS brings together 38 police special intervention units (SIUs) from 27 EU and four external states for the purposes of joint training, equipment and procedural development, as well as cross-border crisis response (Council of the European Union 2017, 1-2). This operational mandate, rooted in EU provisions regarding mutual solidarity in the event of terrorist incidents, was formalised in 2008 and ranges from the provision of equipment to direct on-the-ground support (European Commission 2008, 74). Most recently, the ATLAS Network executed joint operations in Hungary and Belgium, including a 2021 multi-national manhunt for right-wing extremist Jürgen Conings (Europol 2022a, 22). It is important to note, however, that ATLAS does not fall directly under Europol's control. The network is, instead, directly facilitated through funding, materiel, and coordination provided by ECTC's ATLAS Support Office or ASO (Europol "ATLAS Network").

The EU's recognition of CBRN terrorism as an increasingly trans-national challenge has, in turn, pushed the ATLAS Network to engage with CBRN defence through workshops and combined events. Most notably, the network's first cross-border exercise with the ASO in a coordinating role, the 2018 ATLAS Common Challenge, saw French CBRN specialists support German SIUs in stopping a radiological terrorist attack on public transportation (Kelly "Multinational Police Network"). As a network of intervention units, however, ATLAS largely roots its CBRN defence priorities around the tactical resolution of terrorist or criminal incidents in a contaminated environment; far less emphasis is placed on measures such as decontamination, reconnaissance, and monitoring (Simões, 2024). These capabilities would likely incorporate elements from not only law enforcement agencies but civilian authorities, emergency services, and the armed forces as well. Nevertheless, this degree of whole-of-government engagement appears to be largely absent from current CBRN counterterrorism preparations by the network.

2.3. Avenues for NATO Engagement

Opportunities to align the efforts of these Europol bodies with NATO priorities in countering CBRN terrorism are numerous. NATO's own CBRN defence doctrine, Allied Joint Publication (AJP) 3.8, identifies three pillars underpinning its operations: preventing adversaries from acquiring or using CBRN weapons, protecting personnel and territory from existing CBRN threats, and recovering from successful attacks (NATO 2018a, 2-2). At the same time, NATO recognises that adversarial CBRN capabilities, whether state or non-state in origin, do not emerge in a vacuum. Its AJP-3.23 highlights the significance

of “proliferation networks”, supporting infrastructure providing access to CBRN weapons, materiel, or technical expertise (NATO 2023, 5). Disrupting and interdicting these proliferation networks, therefore, represents a key avenue for greater NATO-Europol cooperation in preventive CBRN counterterrorism.

Many proliferation networks leverage existing infrastructure and relations with organised criminal activity to engage in the acquisition or transportation of CBRN materiel. Moldovan authorities in 2015, for instance, uncovered a plot by local smugglers to provide radioactive material sourced from corrupt Russian Federal Security Service officers to Islamic extremists (Meakins “Trafficking in Destruction”). As a hub for law enforcement information-sharing and operational coordination, Europol has already contributed to the fight against these networks, most recently through the role of ECTC and its CBRN-E Team in the 2019 Austrian-Moldovan investigation into nuclear smuggling. Given NATO’s extensive intelligence resources, cooperation with ECTC in identifying and mapping these networks constitutes one potential avenue for enhanced joint engagement in CBRN counterterrorism.

Interestingly, the potential for information-sharing between law enforcement and military bodies is not unprecedented for Europol. In 2018, it deployed a Crime Intelligence Cell (CIC) with the EU Naval Force Mediterranean (EUNAVFOR-MED), a significant initiative which saw Europol provide EUNAVFOR with tailored intelligence to build “reasonable grounds” for interdiction, while sanitizing and disseminating military information to enable action by national police services (Council of the European Union 2018, 26). While the CIC was, itself, centred on intelligence pertaining to migrant smuggling, the project’s success demonstrates the feasibility of information-sharing arrangements between Europol and multi-lateral military organisations.

In addition to intelligence-related activities, cooperation between both organisations could also take form ofon strengthening Europol’s linkages with NATO’s Joint CBRN Defence Centre of Excellence (JCBRN Defence COE). The Centre of Excellence serves as the Alliance’s focal point for CBRN doctrine and capability development and conducts training as well as capacity-building programmes for NATO Allies and partners (NATO “NATO’s Chemical, Biological”). In this latter function, the JCBRN Defence COE’s contribution overlaps with the responsibility of ECTC’s CBRN-E Team to organise instruction for competent authorities in EU Member States, with the potential for closer institutional relations through cross-attendance or joint events.

Most importantly, the JCBRN Defence COE houses NATO’s CBRN Reachback Section, tasked with providing timely analysis and scientific assessments, including the use of advanced modelling and simulation software, to NATO forces as well as external states and organisations (Valenta 2023). ECTC’s CBRN-E Team similarly provides subject-matter expertise to Member State authorities and possesses specific forensic capabilities like conducting post-blast investigations, but its technical assessments remain largely centred on identifying and situating CBRN threats within broader criminal or terrorist modus operandi (Simões 2024). Though real-time scientific reachback falls outside of the ECTC CBRN-E Team’s purview, this overlap of responsibilities between Europol and NATO’s JCBRN Defence COE, again, introduces the possibility for growing rapprochement between both organisations in CBRN counterterrorism.

Finally, NATO possesses unique capabilities in responding to CBRN terrorist incidents. The Alliance, for example, maintains the Combined Joint CBRN Defence Task Force (CJ-CBRND-TF), a multi-national unit comprising a CBRN Joint Assessment Team and CBRND Battalion that can be rapidly deployed in case of armed conflict or at the request of civil authorities (NATO “Combined Joint). NATO also operates a “clearing house mechanism” through the Euro-Atlantic Disaster Response Coordination Centre (EADRCC), allowing members as well as external states and organisations to receive civil and, most notably, military assistance from Member States (NATO “Euro-Atlantic Disaster”). Both entities have already been deployed jointly in the context of CBRN counterterrorism. Most notably, the 2004 Summer Olympics saw the task force stage in Greece to “mitigate the effects” of a CBRN terrorist incident, while the EADRCC acted as the “coordination centre” for a potential Alliance response (Brianas 2004, 35).

The disproportionate psychological impact of CBRN terrorist attacks risks generating mass societal disruption regardless of actual casualties and necessitates, in accordance with NATO’s own guidelines, an “interagency approach for efficient prevention and response” (NATO 2014, 9). As focal points for military and law enforcement cooperation within Europe, both NATO and Europol’s ECTC are uniquely

positioned to serve as joint enablers in the multi-national, whole-of-government engagement which defines CBRN defence. In this sense, the potential for deepened NATO-Europol relations across the full spectrum of CBRN counterterrorism contingencies is both feasible and, amidst an ever-evolving threat environment, increasingly necessary.

2.3.1. The State of Cooperation Today

The current degree of NATO-Europol cooperation in CBRN counterterrorism, however, remains limited. Both NATO and the EU repeatedly affirmed the interconnectedness of their security interests, with their 2018 Joint Declaration calling for "swift and demonstrable" progress in counterterrorism and CBRN defence cooperation (NATO "Joint Declaration"). Relations between NATO and Europol, in turn, slowly developed, with NATO staff first visiting Europol in 2018 to discuss terrorist threats centred on CBRN weapons and improvised explosive devices as well as participating in joint workshops and coordination groups (NATO 2018b, 2). At the same time, informal NATO-Europol ties have also emerged in the counterterrorism field. One 2019 progress report, for instance, highlighted the development of "staff-level" contacts between NATO, the EU, and Europol's ECTC as a notable facet of evolving cooperation (NATO 2019, 3).

Despite these steps, NATO-Europol relations are marked by an overall lack of accompanying institutionalisation. Europol has evaluated avenues for the formalisation of NATO cooperation: the ECTC CBRN-E Team established a strategic partnership with the NATO Counter-IED Centre of Excellence in Madrid, while the agency's 2020-2022 Programming Document called for "the establishment of links with NATO" to enrich its criminal intelligence picture with "strategic information" from military sources (Simões, 2024; Europol 2020a, 42). While some progress has been made, the finalisation of a definitive "working arrangement" remains incomplete as of Europol's latest internal report (Europol 2023c, 109). With this in mind, the paper will now present avenues for deepened cooperation between NATO and Europol in countering the continued threat of CBRN terrorism.

3. Towards Greater NATO-Europol Cooperation

Confronting CBRN terrorism in Europe requires a comprehensive approach, combining both short-term efforts to foster closer tactical and operational relations between NATO and Europol as well as deeper measures aimed at formalising institutional linkages. An initial avenue available to both organisations is, therefore, the development and strengthening of staff-level contacts between NATO, Europol and relevant national authorities.

- **Continued participation in visits and joint forums:** Headquarter visits and workshops were one of the primary facets of NATO-Europol cooperation following the 2018 Joint Declaration between the Alliance and the European Union. Most notably, the former visited Europol to discuss CBRN terrorism and hosted combined seminars on counterterrorism capabilities such as improvised explosive device defeat and CBRN defence. While these events represent a rudimentary form of engagement, their maintenance and, where possible, expansion allow for the sustained staff interactions central to forging long-term trust.

- **Cross-organisational access to databases and platforms:** Both NATO and Europol also maintain an array of integrated databases relevant to CBRN counterterrorism. Platforms such as the ECTC-operated Europol Platform for Experts/European EOD Network allow for direct communication regarding CBRN terrorist incidents and best-practices, strengthening connections between NATO, Europol, and national practitioners regardless of geographic distance. Ensuring cross-organisational access to these systems is, thus, essential and a

key step towards developing greater trust at the tactical and operational levels of CBRN counterterrorism within Europe.

In addition to leveraging existing programmes and initiatives, enhanced NATO-Europol cooperation in CBRN counterterrorism could also centre on forging new partnerships between key sub-organisational units such as NATO's JCBRN Defence COE and ECTC's CBRN-E Team.

- **Establish formal contact between JCBRN Defence COE and ECTC:** The Europol CBRN-E Team Leader strongly emphasised that increased civil-military cooperation with international organisations such as NATO constitutes a key objective for ECTC. In addition to establishing designated points-of-contact in both organisations, JCBRN Defence COE courses represent another avenue for deepened engagement. While civilian law enforcement personnel have attended these programmes, the current degree of Europol involvement is highly limited; formal participation by members of ECTC's CBRN-E Team in NATO courses, in turn, represents an accessible departure point for developing a common understanding of CBRN defence priorities and closer connections between NATO and Europol.

- **Combined Training and Capacity-Building:** The training model adopted by ECTC's CBRN-E Team centres on identifying capability gaps and leveraging existing resources and expertise from within Member States to rectify them. As a military organisation, NATO's JCBRN Defence COE is ideally suited for complex exercises requiring specialised equipment and facilities, including detection, sampling, and decontamination with live CBRN agents. The JCBRN Defence COE could, therefore, work to support Europol's capacity-building efforts through hosting combined training events, further highlighting the potential for deepened NATO-Europol engagement in CBRN counterterrorism.

- **ECTC Membership of CBRN Reachback's Secondary Network:** ECTC has provided strategic and on-the-spot analysis to Member State investigations concerning CBRN substances. Its capabilities, however, remain centred on identifying trans-national threat linkages and common modus operandi, with its team lacking access to capabilities such as real-time modelling and simulation maintained in NATO's CBRN Reachback Section (RBS). The RBS, however, operates a Secondary Network, consisting of organisations and institutions who provide CBRN defence information and assistance and, in turn, can task the section for support if required. The integration of ECTC's CBRN-E Team into the Secondary Network, thus, constitutes a mutually beneficial relationship in CBRN counterterrorism: the RBS could leverage Europol information and analysis on emerging CBRN hazards within the criminal or terrorist sphere, while ECTC would possess timely access to scientific and technological enablers found nowhere else within its organisation.

Ultimately, the potential for deepened cooperation between NATO and Europol extends beyond the role of the JCBRN Defence COE, with the operational exigencies of CBRN counterterrorism introducing new avenues for sustained engagement between both organisations.

- **ECTC and ATLAS Network Participation in NATO Crisis Response Exercises:** As central pillars of European military and police cooperation, NATO and Europol are uniquely positioned to enable the cross-border and cross-sectoral cooperation required in a CBRN counterterrorism response. This degree of engagement, however, cannot be generated in an emergency and must be developed prior to crises. Annual exercises by NATO's EADRCC, testing the preparedness of states and organisations in scenarios such as terrorist chemical attacks, represent one avenue for achieving this (Jacuch 2017, 172). Participation by ECTC's CBRN-E Team or ATLAS Support Office would allow Europol to practice enabling law enforcement information sharing and coordination within a truly inter-agency environment, while also building familiarity between European police services and the multi-national military assets they may operate alongside in responding to CBRN terrorist incidents.

- **Finalising a NATO-Europol Working Arrangement:** The continued involvement of organised crime in violent non-state actor efforts to acquire and develop CBRN capabilities highlights the growing nexus between internal and external security priorities and institutions. As vital nodes in the exchange of security information within Europe, NATO and Europol possess extensive collection and analysis capabilities needed to effectively monitor this challenge; despite ongoing efforts, however, no formal information-sharing agreements exist between both organisations. Finalising a NATO-Europol working arrangement, thus, constitutes a key long-term objective, allowing for the fusion of criminal intelligence with strategic information from the Alliance to improve situational awareness and assist Member State military or law enforcement in detecting and countering CBRN terrorist threats before they can materialise.

4. Conclusion

The CBRN threat picture today is defined by constant transformation, as a growing array of adversarial actors and capabilities challenge long-held understandings of CBRN terrorism as limited in scope, scale, and likelihood. Jihadist and violent right-wing groups, though still the predominant extremist threat in Europe, are increasingly joined by single-issue movements and hostile states as likely perpetrators of future CBRN attacks. At the same time, technological advancements, ranging from large language models to unmanned vehicles, have significantly augmented the accessibility and lethality of CBRN weapons, allowing even lone actors to inflict greater casualties and, perhaps most significantly, mass disruption.

Both NATO and the European Union recognise this strategic challenge largely surpasses the capacities of any single state, necessitating a multi-lateral and multi-sectoral response comprising civilian institutions, law enforcement, and the armed forces. As cornerstones of European military and police cooperation, NATO and Europol are vital in enabling this cooperation. While the degree of formalised engagement between both institutions has, thus far, been limited, this report identifies seven avenues to rectify this partnership gap.

The first five comprise short and medium-term measures intended to strengthen institutional relations in CBRN counterterrorism. They include developing staff-level contacts through continued headquarter visits and participation in joint forums; ensuring cross-organisational access to relevant databases; and formalising a partnership between NATO's JCBRN Defence COE and Europol's CBRN-E Team through course attendance, combined training events, and Europol membership of the JCBRN Defence COE's Secondary Reachback Network. Two final measures reflect the potential for deeper, enduring linkages between both organisations. In addition to encouraging Europol participation in NATO crisis response exercises centring on CBRN terrorist incidents, the finalisation of a NATO-Europol working arrangement would significantly enhance joint efforts to proactively detect and counter CBRN threats.

2024 marked a significant moment for NATO and Europol, as they celebrated their 75th and 25th anniversaries respectively. Though founded 50 years apart to counter differing threats, both organisations are driven by a common force, captured by Europol's Executive Director earlier this year: "every operation we undertake, every partnership we forge, and every innovation we embrace is ultimately aimed at ensuring the safety and security of our communities" (Europol "25 Years"). The threat of CBRN terrorism is, ultimately, irreducible. Nevertheless, it is by fostering cooperation between NATO and Europol on the basis of this shared objective that the European community best equips itself to confront current and emerging security challenges.

Authors and Acknowledgements

Author

Mathias KATSUYA is a final-year undergraduate student of International Relations at the University of St Andrews in Scotland. He completed an internship with the Joint CBRN Defence Centre of Excellence in 2024 and previously worked for the George C. Marshall European Center for Security Studies as both an intern and adjunct. Mathias' interests largely focus on counterterrorism and irregular warfare, particularly regarding civil-military cooperation in addressing emerging strategic threats.

Author's Acknowledgement - *This report would not have been possible without the contributions of numerous external subject-matter experts. I would like to thank the military and civilian staff of the Joint CBRN Defence Centre of Excellence, including Tomaš Michalčik and Lucie Sedláčková, for their guidance and continued support through informal interviews and conversations. I am also grateful to the European Counter Terrorism Centre and João Simões, whose first-hand insights as Europol's CBRN-E Team Leader were central to shaping the product of this final report.*

Supervisor

Tomáš MICHALČÍK is the Outreach Coordinator at the Joint Chemical, Biological, Radiological and Nuclear Centre of Excellence, where he is responsible for engagement with external partners, such as the European Union, Academia, or Partner nations. A Master's graduate in War and Peace Studies from Palacký University, Tomáš has a strong foundation in Transatlantic security, honed through roles such as his tenure at the Czech Embassy in Helsinki during Finland's NATO accession process. Aditionally, Tomáš also leads the planning and organization of the JCBRN Defence COE Annual Conference, which brings together CBRN Defence Experts from NATO and its partners.

Bibliography

Acton, James, M. Brooke Rogers, and Peter Zimmerman. 2007. "Beyond the Dirty Bomb: Re-Thinking Radiological Terror." Survival: Global Politics and Strategy 49 (3): 151–68. https://doi.org/10.1080/00396330701564760.

Ananthan, Rueben, and Santhana Dass. 2021. "Jihadists' Use and Pursuit of Weapons of Mass Destruction: A Comparative Study of Al-Qaeda and Islamic State's Chemical, Biological, Radiological and Nuclear (CBRN) Weapons Programs." Studies in Conflict & Terrorism 47 (5): 548–82. https://doi.org/10.1080/1057610x.2021.1981203.

Bellingcat. Published April 20, 2021. "Senior GRU Leader Directly Involved with Czech Arms Depot Explosion." https://www.bellingcat.com/news/2021/04/20/senior-gru-leader-directly-involved-with-czech-arms-depot-explosion/.

Bensahel, Nora. 2003. The Counterterror Coalitions: Cooperation with Europe, NATO, and the European Union. Santa Monica: RAND Corporation. https://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR1746.pdf.

Bernasconi, Claudia. 2011. "NATO's Fight against Terrorism: Where Do We Stand?" NATO Defense College Research Paper, no. 66: 1–8. https://www.files.ethz.ch/isn/128562/rp_66.pdf.

Bleek, Philipp, and Zachary Kallenborn. 2018. "Avatars of the Earth: Radical Environmentalism and Chemical, Biological, Radiological, and Nuclear (CBRN) Weapons." Studies in Conflict & Terrorism 43 (5): 351–81. https://doi.org/10.1080/1057610x.2018.1471972.

Bolanos, Alejandro. 2014. "Yes: The 'New Terrorism' or the 'Newness' of Context and Change." In Contemporary Debates on Terrorism, edited by Richard Jackson and Justin Sinclair, 29–35. London: Routledge.

Bossong, Raphael. 2018. "Intelligence Support for EU Security Policy: Options for Enhancing the Flow of Information and Political Oversight." SWP Comment, no. 51: 1–8. https://www.swp-berlin.org/publications/products/comments/2018C51_Bsg.pdf.

Brianas, Jason. 2004. NATO, Greece, and the 2004 Summer Olympics. Monterey: Naval Postgraduate School. https://apps.dtic.mil/sti/tr/pdf/ADA429691.pdf.

Bures, Oldrich. 2008. "Europol's Fledgling Counterterrorism Role." Terrorism and Political Violence 20 (4): 498–517. https://doi.org/10.1080/09546550802257218.

Carus, Seth. 2000. "R.I.S.E." In Assessing Terrorist Use of Chemical and Biological Weapons, edited by Jonathan Tucker, 55–70. Cambridge: Belfer Center for Science and International Affairs.

Cetina, Ivana, and Jugoslav Jozić. 2022. "Impact of the New Technologies on CBRN Terrorist Threats: General Perspective and Perspective of Republic of Croatia." Vojenské Rozhledy 4: 119–39. https://doi.org/10.3849/2336-2995.31.2022.04.119-139.

Cordova, Kimberlee, Kevin Esvelt, Rafael Rocha, Emily Soice, and Michael Specter. 2023. Can Large Language Models Democratize Access to Dual-Use Biotechnology?" Ithaca: Cornell University. Accessible from: https://arxiv.org/abs/2306.03809.

Council of the European Union. 2017. Strengthening the ATLAS Network. Brussels: Council of the European Union. Accessible from: https://www.statewatch.org/media/documents/news/2017/sep/eu-council-atlas-network-11828-17.pdf.

———. 2018. Crime Information Cell Pilot Project Final Report. Brussels: Council of the European Union. Accessible from: https://www.asktheeu.org/es/request/10928/response/38280/attach/5/Crime%20Information%20Cell%20Pilot%20Project%20redacted.pdf?cookie_passthrough=1

Counter Terrorism Policing. Published September 28, 2023. "Man Found Guilty of Terror Charge after Building Drone to Give to ISIS." https://www.counterterrorism.police.uk/man-found-guilty-of-terror-charge-after-building-drone-to-give-to-isis/.

Deflem, Mathieu. 2006. "Europol and the Policing of International Terrorism: Counter-Terrorism in a Global Perspective." Justice Quarterly 23 (3): 336–59. https://doi.org/10.1080/07418820600869111.

Devoic, Bozenko. 2012. The Post-9/11 European Union Counterterrorism Response: Legal-Institutional Framework. Monterey: Naval Postgraduate School.

DG HOME. 2017. Action Plan to Enhance Preparedness against Chemical, Biological, Radiological and Nuclear Security Risks. Brussels: European Commission. Accessible from: https://home-affairs.ec.europa.eu/system/files/2020-09/20171018_action_plan_to_enhance_preparedness_against_chemical_biological_radiological_and_nuclear_security_risks_en.pdf.

Dolzikova, Darya. Published September 18, 2023. "Degradation Everywhere: The Long-Term Risks at Ukraine's Zaporizhzhia Plant." https://www.rusi.org/explore-our-research/publications/commentary/degradation-everywhere-long-term-risks-ukraines-zaporizhzhia-plant.

European Commission. 2002. Council Decision 2003/48/JHA on the Implementation of Specific Measures for Police and Judicial Cooperation to Combat Terrorism in Accordance with Article 4 of Common Position 2001/931/CFSP. Brussels: European Commission. Accessible from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003D0048.

———. 2008. Council Decision 2008/617/JHA on the Improvement of Cooperation between the Special Intervention Units of the Member States of the European Union in Crisis Situations. Brussels: European Commission. Accessible from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0073:0075:EN:PDF.

———. 2016. Communication from the Commission to the European Parliament, the European Council and the Council Delivering on the European Agenda on Security to Fight against Terrorism and Pave the Way towards an Effective and Genuine Security Union. Brussels: European Commission. Accessible from" https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016DC0230.

European Counter Terrorism Centre. Published July 7, 2021. "The Threat of Violent Left Wing & Anarchist Extremism in the EU." https://www.icct.nl/sites/default/files/import/publication/eu-europol-violent-left-wing-anarchist-extremism-presentation-7-7-21.pdf.

Europol. 2011. European Bomb Data System. Brussels: Publications Office of the European Union. Accessible from: https://op.europa.eu/en/publication-detail/-/publication/e60d364e-c153-416f-94c2-a37d0927ca87.

———. 2017. European Union Terrorism Situation and Trend Report - 2017. The Hague: Europol. Accessible from: https://www.europol.europa.eu/sites/default/files/documents/tesat2017.pdf.

———. 2018. European Union Terrorism Situation and Trend Report - 2018. The Hague: Europol. Accessible from: https://www.europol.europa.eu/cms/sites/default/files/documents/tesat_2018_1.pdf.

———. Published March 12, 2019. "European Counter Terrorism Centre – ECTC https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc.

———. Published December 6, 2019. "Crime Group Suspected of Smuggling Nuclear Materials Arrested in Vienna." https://www.europol.europa.eu/media-press/newsroom/news/crime-group-suspected-of-smuggling-nuclear-materials-arrested-in-vienna.

———. 2020a. Consolidated Annual Activity Report 2019. The Hague: Europol. Accessible from: https://www.europol.europa.eu/cms/sites/default/files/documents/consolidated_annual_activity_report_2019.pdf.

———. 2020b. Europol Programming Document 2020-2022. The Hague: Europol. Accessible from: https://www.europol.europa.eu/cms/sites/default/files/documents/europol_programming_document_2020-2022.pdf.

———. 2022a. Consolidated Annual Activity Report 2021. The Hague: Europol. Accessible from: https://www.europol.europa.eu/cms/sites/default/files/documents/Consolidated%20Annual%20Activity%20Report%202021.PDF.

———. 2022b. European Union Terrorism Situation and Trend Report - 2022. The Hague: Europol. Accessible from: https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf.

———. 2023a. Consolidated Annual Activity Report 2022. The Hague: Europol. Accessible from: https://www.europol.europa.eu/cms/sites/default/files/documents/Consolidated%20Annual%20Activity%20Report%202022.PDF.

———. 2023b. European Union Terrorism Situation and Trend Report - 2023. The Hague: Europol. Accessible from: https://www.europol.europa.eu/cms/sites/default/files/documents/European%20Union%20Terrorism%20Situation%20and%20Trend%20report%202023.pdf.

———. 2023c. Europol Programming Document 2024-2026. The Hague: Europol. Accessible from: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Programming_Document_2024-2026.pdf.

———. 2023d. The European Union Agency for Law Enforcement Cooperation in Brief. The Hague: Europol. Accessible from: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20in%20Brief.pdf.

———. Updated April 12, 2023. "ATLAS Network.". https://www.europol.europa.eu/partners-collaboration/atlas-network.

———. Published April 24, 2023. "Europol Analysis Projects.". https://www.europol.europa.eu/operations-services-innovation/europol-analysis-projects

———. Updated August 11, 2023. "About Europol.". https://www.europol.europa.eu/about-europol.

———. Updated August 18, 2023. "Operational and Analysis Centre." https://www.europol.europa.eu/about-europol/operational-and-analysis-centre.

———. Updated May 7, 2024. "Statistics & Data." https://www.europol.europa.eu/about-europol/statistics-and-data.

———. Published May 28, 2024. "25 Years of Making Europe Safer – Europol Anniversary." https://www.europol.europa.eu/media-press/newsroom/news/25-years-of-making-europe-safer-europol-anniversary.

Fade, Florian. 2018. "The June 2018 Cologne Ricin Plot: A New Threshold in Jihadi Bio Terror." CTC Sentinel 11 (7): 1–4. https://ctc.westpoint.edu/wp-content/uploads/2019/01/CTC-SENTINEL-082018-final.pdf.

Ferguson, Charles, William C Potter, and Amy Sands. 2005. The Four Faces of Nuclear Terrorism. London: Routledge.

Fleer, BreAnne. 2020. "Radiological-Weapons Threats: Case Studies from the Extreme Right." The Nonproliferation Review 27 (1-3): 225–42. https://doi.org/10.1080/10736700.2020.1775987.

GI-TOC. 2024. Smoke on the Horizon: Trends in Arms Trafficking from the Conflict in Ukraine. Geneva: Global Initiative Against Transnational Organized Crime. Accessible from: https://globalinitiative.net/wp-content/uploads/2024/06/Smoke-on-the-horizon-trends-in-arms-trafficking-from-the-conflict-in-Ukraine-GI-TOC-June-2024.v3.pdf

Grady, Broderick. 2002. "Article 5 of the North Atlantic Treaty: Past, Present, and Uncertain Future." Georgia Journal of International and Comparative Law 31 (1): 167–98. https://digitalcommons.law.uga.edu/gjicl/vol31/iss1/10.

Hoffman, Bruce. 2009. "The First Non-State Use of a Chemical Weapon in Warfare: The Tamil Tigers' Assault on East Kiran." Small Wars & Insurgencies 20 (3-4): 463–77. https://doi.org/10.1080/09592310903026969.

Human Rights Watch. Published May 1, 2017. "Death by Chemicals: The Syrian Government's Widespread and Systematic Use of Chemical Weapons." https://www.hrw.org/report/2017/05/01/death-chemicals/syrian-governments-widespread-and-systematic-use-chemical-weapons.

Hummel, Stephen. 2016. "The Islamic State and WMD: Assessing the Future Threat." CTC Sentinel 9 (1): 18–21. https://ctc.westpoint.edu/wp-content/uploads/2016/01/CTC-SENTINEL-Vol9Iss13.pdf.

Jacuch, Andrzej. 2017. "NATO's Involvement in Humanitarian Operations/Disaster Response." Przegląd Nauk O Obronności 1 (4). https://doi.org/10.5604/01.3001.0013.0118.

Jenkins, Brian. 1985. International Terrorism: The Other World War. Santa Monica: RAND Corporation. https://apps.dtic.mil/sti/pdfs/ADA163576.pdf.

Kaunert, Christian. 2010. "Europol and EU Counterterrorism: International Security Actorness in the External Dimension." Studies in Conflict & Terrorism 33 (7): 652–71. https://doi.org/10.1080/1057610x.2010.484041.

Kelly, Fergus. Published October 11, 2018. "Multinational Police Network ATLAS Conducts 7 Counter-Terror Exercises across Europe." https://www.thedefensepost.com/2018/10/11/multinational-atlas-network-counter-terror-exercises-europe-police/?utm_content=cmp-true#google_vignette.

Koehler, Daniel, and Peter Popella. 2018. "Mapping Far-Right Chemical, Biological, Radiological, and Nuclear (CBRN) Terrorism Efforts in the West: Characteristics of Plots and Perpetrators for Future Threat Assessment." Terrorism and Political Violence 32 (8): 1666–90. https://doi.org/10.1080/09546553.2018.1500365.

König, Franca, and Florian Trauner. 2021. "From Trevi to Europol: Germany's Role in the Integration of EU Police Cooperation." Journal of European Integration 43 (2): 175–90. https://doi.org/10.1080/07036337.2021.1877694.

Meakins, Joss. Published September 5, 2017. "Trafficking in Destruction: Nuclear Smuggling in the Black Sea Region." https://rusi.org/networks/shoc/informer/trafficking-destruction-nuclear-smuggling-black-sea-region#:~:text=Moldova%20is%20another%20important%20node.

Meulenbelt, Stephanie, and Maarten Nieuwenhuizen. 2015. "Non-State Actors' Pursuit of CBRN Weapons: From Motivation to Potential Humanitarian Consequences." International Review of the Red Cross 97 (899): 831–58. https://doi.org/10.1017/s1816383116000011.

Morgan, Matthew. 2004. "The Origins of the New Terrorism ." Parameters 34 (1): 29–43. https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2190&context=parameters.

NATO. 2014. Non-Binding Guidelines for Enhanced Civil-Military Cooperation to Deal with the Consequences of Large-Scale CBRN Events Associated with Terrorist Attacks. Brussels: NATO Defence Policy & Planning Division.

———. 2018a. Allied Joint Doctrine for Comprehensive Chemical, Biological, Radiological, and Nuclear Defence. Brussels: NATO Standardization Office.

———. 2018b. Third Progress Report on the Implementation of the Common Set of Proposals Endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017. Brussels: NATO. Accessible from: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_06/20180608_180608-3rd-Joint-progress-report-EU-NATO-eng.pdf.

———. Published July 10, 2018. "Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization." https://www.nato.int/cps/en/natohq/official_texts_156626.htm.

———. 2019. Fourth Progress Report on the Implementation of the Common Set of Proposals Endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017. Brussels: NATO. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_06/190617-4th-Joint-progress-report-EU-NATO-eng.pdf

———. Updated September 20, 2021. "Euro-Atlantic Disaster Response Coordination Centre." https://www.nato.int/cps/en/natohq/topics_52057.htm?.

———. Updated April 13, 2022. "Combined Joint Chemical, Biological, Radiological, and Nuclear (CBRN) Defence Task Force." https://www.nato.int/cps/en/natohq/topics_49156.htm#:~:text=NATO's%20Combined%20Joint%20CBRN%20Defence%20Task%20Force%20(CJ%2DCBRND%2D,NATO%20populations%2C%20territory%20or%20forces..

———. Updated July 5, 2022. "NATO's Chemical, Biological, Radiological and Nuclear (CBRN) Defence Policy." https://www.nato.int/cps/en/natohq/official_texts_197768.htm.

———. 2023. Allied Joint Doctrine for Countering Weapons of Mass Destruction in Military Operations. Brussels: NATO Standardization Office.

NATO Standardization Office. 2016. "Terrorism." https://nso.nato.int/natoterm/Web.mvc

Parachini, John. 2005. "Aum Shinrikyo." In Aptitude for Destruction, Volume 2: Case Studies of Organizational Learning in Five Terrorist Groups, edited by John Baker, Peter Chalk,

Kim Cragin, Brian Jackson, John Parachini, and Horacio Trujillo, 11–36. Santa Monica: RAND Corporation. Accessible from: http://www.jstor.org/stable/10.7249/mg332nij.9..

Pauwels, Annelies. 2021. Contemporary Manifestations of Violent Right-Wing Extremism in the EU: An Overview of P/CVE Practices. Brussels: European Commission. Accessible from: https://home-affairs.ec.europa.eu/document/download/98e71d43-b493-4d60-ad05-e2dea2930a33_en?filename=ran_adhoc_cont_manif_vrwe_eu_overv_pcve_pract_2021_en.pdf**.**

Simões, João, interview by Mathias Katsuya, June 27, 2024.

Sin, Steve and Markus Binder. 2022. Violent Non-State Actor Chemical, Biological, Radiological, and Nuclear (VNSA CBRN) Event Database, Version 1.0. College Park: University of Maryland Asymmetric Threats Analysis Center, National Consortium for the Study of Terrorism and Responses to Terrorism Unconventional Weapons & Technology Division.

Spencer, Alexander. 2006. "Questioning the Concept of 'New Terrorism.'" Peace, Conflict & Development, no. 8: 1–33. https://epub.ub.uni-muenchen.de/13769/1/Feb%2006%20SPENCER%20version%202.pdf.

Tu, Anthony. 2020. "The Use of VX as a Terrorist Agent: Action by Aum Shinrikyo of Japan and the Death of Kim Jong-Nam in Malaysia: Four Case Studies." Global Security: Health, Science and Policy 5 (1): 48–56. https://doi.org/10.1080/23779497.2020.1801352.

Valenta, Petr. 2023. "CBRN Reachback Activities." JCBRN Defence COE Newsletter, no. 19. https://www.jcbrncoe.org/index.php?option=com_content&view=article&id=702.

Weiss, Michael. Published August 15, 2023. "Blood Simple. Several Russian Journalists and Activists Were Poisoned in Europe." https://theins.ru/en/politics/264280**.**

.

ANNEX A: A Conversation with João Simões (Europol CBRN-E Team Leader)

*This transcription has been edited for clarity

Mathias Katsuya (MK): So, I suppose the best way to start would just be to hear a little bit about where the CBRN-E team sits within ECTC, because I know there's not much out there regarding actual departments and the structure within it.

João Simões (JS): Europol has many departments. We have cyber, we have a financial/economic crime, and we also have CT (counterterrorism), among others. Within the ECTC, there are three units, and mine in the structure would be the first unit. The unit is called “Expertise and Stakeholder Management”, and within this unit there is one team that deals on CBRN-E topics.

Even though we are with the ECTC, we are a technical team. We don't cross check names, for instance; we have other teams [called] Analysis Projects (AP) that do this. The “AP” (Analysis Projects), [and] AP Weapons and Explosives is overlapped with ours, and they are the ones that have the analysts and do the cross-check of people, for instance. If a member state asks us to run to cross-checks on a suspect against Europol databases, they do it.

Our team, the CBRN and explosive team just do the technical part, so we conduct technical assessment on devices, MO (modus operandi), we try to identify patterns, trends. Because we are technical team, even though we are within the ECTC, we are a horizontal team […] we don't focus so much on the reason why the attack happened. We have other teams for right wing, left wing, religious motivated terrorism. And because we don't focus so much on the reason why, we also assist serious and organized crime investigations and property crime, property crime being when explosive is used, for instance, to conduct ATM attacks.

MK: So, the team itself, it's almost like a bit of a service provider to the other departments within the agency as a whole?

JS: Yeah, everyone that needs assistance when it comes to explosive or CBRN substances, regardless of in which department they are focused on, we can provide our technical assistance of course.

MK: In terms of the composition of the team, I know your background for instance is with the Portuguese government on the EOD side, but you also have obviously some CBRN knowledge is the team itself. Is everyone more or less dual-hatted, as in everyone is an EOD tech and a CBRN specialist, or are there, you know, segments within the team that focus more on one or the other?

JS: Yeah. So, for starters, we are a small team. This means that it facilitates how we, spread and divide the work, in which you have the team leader and then half of the Team that focus on explosive, and the other half focuses on CBRN. This is the general structure of the team.

However, to join the team, even though we have CBRN from one side [and] EOD and IEDD from the other, we are all bomb techs. So, this is a must. And all of us have CBRN training as well [as] first responders, so we don't have CBRN forensics – we don't work in the lab. All of us need to have CBRN training as a first responder in our national governments, but then in-house, there are people that focus more on CBRN because they like it more and others that focus on the explosive parts.

Myself, I have both. I tend to like more CBRN because I think it's more challenging, so that's why I started to study a bit more on the CBRN side. But we all need to be also bomb techs; a prerequisite to join the team is to be a bomb technician.

MK: And in general, then, you're seconded from your national governments to Europol?

JS: Depends. We have two types within our team, we have two types of contracts: SNE, which is a Seconded National Expert, , in which the country still pays your salary,. And then we also have TA, temporary agents. This my case now.

I started as an SNE, and so the Portuguese police, gave permission for me to be here. I can still be promoted while I'm here - but I don't have any allowance from the Portuguese. I'm Europol staff, so everything is from Europol.

This means that the big difference I would say is that SNEs, because your government still pays for your allowance, they kind of are entitled to, if they need you next week, you have to go back.

On the contrary, TAs, because you are at 100% Europol staff, the government cannot ask you to go back next week.

MK: I noticed that you mentioned that the team [is] on the technical side. You don't focus for instance, on the forensics of CBRN or IED or explosive threats.

JS: So, we do forensics as in post-blast investigations (PBI), so this would be forensics, but we don't do analytical chemistry. We don't have that expertise. We have chemists within our team, but as we don't have a lab, we don't do this part. But we do cross check MOs [modus operandi], so this can be included in the investigation, but not so much scientific forensics.

When it comes to explosives, we do post blast investigation, and Member States can ask us to go and assist them in the investigation.

MK: So, the main reason I ask that is because here at the COE, we have a dedicated Reachback Section, which focuses obviously on that scientific and that technical expertise and simulation and modelling. Do you have that capability at all within the CBRN team or within the analytical projects, or is that something that's outside the organisation's purview?

JS: When you say Reachback, I don't know exactly what type of reachback capabilities you have. Is it live reachback if someone needs it?

MK: Yeah, it's live reachback. It's real time.

JS: OK, so we don't have that. Let’s keep in mind that, when we talk about European countries, everyone is very well prepared, I would say. So, when we engage with the countries, it's not so much because they need our technical assistance on the device itself or in the CBRN substance. It's more because they want to understand if this is also happening in other countries.

Or sometimes they want, for instance, if when you go to the doctor, sometimes you want to have a second opinion. This is why sometimes countries also asks us. So not so much for the reachback capabilities, the enhanced knowledge on specific chemical or bioagent or whatever, but more for confirmation of what they found and also to see patterns.

We don't have the live [reachback] simply because we are a small team; we don't have capability to provide this service to the member states. What we do have still, it's a 24-hour service, so if the members need us as soon as possible, we have a 24/7 office, and if there's a call for CBRN incidents, they can call me at 3:00 AM for instance. But it's not that we can provide this assistance immediately, you know?

MK: Yeah, the main reason was I wanted to gain a better understanding of the team and its capabilities. I know you also have a mandate to provide on-the-spot technical assistance to member states. I think there was a case, I think it was in 2019, [involving] nuclear smuggling. I know that we're getting perhaps into some into slightly sensitive areas, but to the extent that you can, [could you] touch on what are your team's capabilities in providing that more on-the-spot assistance to investigations.

JS: As I said before, we can be deployed for investigations. We have a strategic component, and we have an operational one, and [this] operational one is the reason why we exist. We usually divide operational assistance in two areas.

One is while we are sitting here in the office in The Hague, where HQ is, and countries send us cases, we provide our technical assistance [or] technical report on the substance. But also countries might request our deployments on-the-spot to assist in many different fields.

The case that you're mentioning was on open sources, so it's OK - on the Europol website, you can also see the video. It involves Austria and Moldova, and the arrest took place in Vienna in 2019. Essentially the reason why we were deployed to that case, [is] it was a CBRN case – rad/nuc - in which someone was allegedly trying to sell a nuclear substance.

Our deployment was for the CBRN part [and] also for everything else around it. It was an investigation that was started here at Europol. Many meetings took place, many things were ongoing, and this staff member was always involved. So, he was also present in the arrest phase, and he provided his opinion of course – [you can] seen in the video they use detectors there - so he was also there to provide his operation on the experience.

But this case, contrary to the cases for post-blast investigation where we actually stay one month in the country for the investigation or assist countries in the forensic part, we didn't assist in the CBRN investigation part. The substance was sent to the labs, and the labs then provided their reports.

MK: So, the presence in cases that generally aren't, for instance, post-blast or post-incidents, it's generally more of that culmination of the investigative process that's involves Europol.

JS: Yes, when we are deployed we have a mobile office, in which he had on-the-spot access to all of the Europol databases. This means that if they found something odd, he could immediately check if, in our systems, we had something similar. This was also his role in this investigation, not just the final culmination with the arrest, but also by having the mobile office with him with access to all of our systems - he also provided this this expertise to the Austrian colleagues.

MK: And because I know you mentioned the systems, is one of them the EBDS, the European Bomb Data System?

JS: Yeah, EBDS is one, it's a secure system and usually it's not directly connected to the bomb techs units. On the contrary, we have one which is called EPE – Europol Platform for Experts/EEODN. EEODN stands for European EOD Network […] it essentially is the European network for bomb techs and CBRN specialists.

There are many networks on the European level for law enforcement. and if you Google, you will find many of them. The most popular, I would say, is the ATLAS Network, which is for special intervention units. But the EEODN is a network created in 2008. Estonia is currently the chair, but we act as the secretariat; we are like this elephant memory that always remains with the with the network. And this network has an online platform, so this is one of the systems. It's not just a database, and there's also a forum [where] people can discuss among themselves whatever they would like, but [they] cannot use personal data […] we cannot use names, but we can use technical terms for devices.

And then in-house, you have other systems that collect info, but they are not directly reachable by the member states. So, this one, EPE/EODN, they can go on directly, [but for] the others usually they send to us, we run the information in our systems, and then we feedback the information.

MK: And in those cases, that's why it's useful for instance, to have a member of the team on the ground there to assist.

JS: Yeah, usually EU MS cannot have direct access, is quite simple. It's personal data, classified information sometimes, and Europol [doesn't have] the data. So imagine there is a case in Portugal, my country, as you know. If there's a case in Portugal, Portuguese authorities, contribute to Europol saying there was a trafficking of radiological substance. And then they can put a handling code, and the handling code is where they define to whom this information can be shared. Sometimes they say: to be shared only with Europol.

So, if this is the case, for instance, my colleague was deployed in Austria, [and] in the system, he would check, OK, there's a contribution from Portugal on this. He could not inform the Austrian authorities

without the permission from the Portuguese authorities because they said only to be shared with Europol. So that's why the countries don't have direct access. First, we need to request [it from] Portugal, that [due to an] ongoing case, we would like you to lift the handling code to be shareable with other member states. And then we make this happen, this link.

Usually because the investigations are ongoing, and every now and again, law enforcement authorities need to ask the judge that this information is released to other member states. This is why they don't have direct access to the members.

MK: No, that makes sense. And then your role is to function as that conduit between the different states. Just touching on the different systems in the databases, because I know for EBDS and then also for the European EOD network that law enforcement is the main stakeholders in the networks. Are they also open, for instance, to national military EOD and CBRN units as well?

JS: Actually, the term that we use is not law enforcement; we actually use “competent authorities” in the field of CBRN and explosives. And there are many cases in which the units involved are military units. For instance, in the Netherlands the police don't have EOD, so it's the military that takes over. In Belgium, it’s the same. Ireland is the same.

These units there are competent authorities according to the national law or internal [frameworks]. If they are considered as competent authorities to act by their countries, for us, they are also competent authorities to deal with cases. To that end, they are also part of the network, and they join our activities.

We just had one that finished two weeks ago in Estonia, and the Belgium EOD and the Dutch EOD, they were instructors and also trainees. We have it also that some of the units are even civil protection, for instance in Estonia; in Estonia, the EODs are from the rescue board, […] in France, their unit is “Deminage”, which is also civil protection. So that's why we try to avoid the law enforcement term, and we use competent authorities.

MK: So, you just mentioned the training events that you hold. I know that's one of the responsibilities on the team, hosting or organising those training events. What role do you play in that specifically, or do you just organize the events you participate in and the instruction as well?

JS: So, the whole cycle [is] usually every two years, in which we ask member states, what are your training needs? What are your training capabilities in terms of facilities and what are your training capabilities in term of instructors? For instance, Portugal would answer, we need training on radiation detection, [but] we have a very good blasting range and a very good capability in terms of forensics. So, we collect all of this information, and then we try to put it together: OK, this is what they need. This is what we have in terms of facilities and what we have in terms of expertise.

What we do then is try to have the expert from Portugal going to the training in Finland (e.g.) as a trainer and put together that training package according to the most requested training needs

Our role here is to identify the training gaps, the best trainers, the best facilities, [trying] to be creative in terms of budget allocation. This is also very challenging - trying to find the best budget line to make these trainings happen. And then we use the official channels to invite everyone when the training is deployed.

We also participate as trainers. What we usually do, I told you we have experts on specific topics, […] Still, we always try to have member states trainers, but usually at the beginning of the session, we always […] put everyone on the same page in terms of what's the threat, to provide everyone with a current threat assessment.

MK: And those threat assessments, do you produce them? Because you mentioned the CBRN-E Team is more on the technical side, is that something that you produce, or is it the analytical projects that are responsible for those?

JS: So how it works, for instance, is we have an AP Check the Web - as the name says, they check the web, they check everything that is online. The threat assessment essentially [is a] sum of the intention and the capabilities, and then we have the threat. For the intention, what we see very clearly is that what

is being disseminated online is what we see happening in actual cases. So, it's happening on the ground; we know that there is a direct link

AP Check the Web [conducts] an extensive open-source monitoring, and whenever they find anything relevant [to] CBRN and explosives, they send it to us. And then we assess it, for instance, [as] “oh no, this is just a kid’s joke. This is not feasible. It’s nothing or this is something.”

If we see that it's something but it's not new, we [keep] it for ourselves, and we feed this threat assessment – “there was an increase in whatever”. If we see there is something relevant and new, we inform immediately the member states [and] every now and again, if we see that something new and potentially dangerous, we also conduct experiments before informing the member states

This usually happens mainly on the explosive [side] because it's easier for us to test new recipes for explosives. On CBRN, this also happens, but for that, because I told you we don't have labs, we liaise with some agencies that do have labs. One of our main partners is the JRC - the Joint Research Centre. They belong to the European Commission, and […] there have multiple labs, one for nuclear forensics, some for explosives. So, our threat assessment, essentially, is a compilation of what we find online with a mix of what we find on the ground, and then we put together the threat assessment.

Of course, even though we don't have analysts, we are capable of doing it ourselves […] also because there [are not so many] CBRN cases. So, this allows us to put together a good picture, but to have a bigger network […] we rely on the other AP teams to feed us with the cases, with property crime cases, with the serious organized crime cases, and with terrorism cases.

MK: For those APs then, are they assigned to specific centres like ECTC or are they housed somewhere else worth within Europol?

JS: Yeah, they are also [within ECTC]. So Check the Web, for instance, is within the ECTC because it was initially focusing on jihadist terrorism [when] all the propaganda was very active. […] Weapons and Explosives, they are under the SOCs (Serious Organised Crime), and we have an excellent cooperation with them.

As for terrorism, probably, you know, it's mostly improvised things. For organized crime, not so much. It's usually proper hand grenades, proper ordinances or military ordinances that are used, so this is also good for us to see. This is in the market that could potentially be used for terrorism as well.

MK: It's interesting because it seems like you and the team, at least, are very well positioned to draw from all the different threat streams that Europol focuses on.

JS: Well, we, again, are a technical team, so whenever the other APs need our assessments, we assist them. The ultimate goal is to provide better assistance to the member states. So, the member states have a case, and the team focuses on the cross-check, to check if ‘Joao’ has any hit in our system or provides any hit in our system. Other teams focus on the intelligence package, so they go through my social media platforms, try to identify all of my Internet fingerprint, for instance, […] to increase this intelligence packets for the countries. If it's related to explosive, we also provide a, technical assessment on the explosive.

MK: I suppose this is a good part to segue into your engagements not only within Europol’s other departments and analytical projects but also outside of Europol. I know that there has been some contact historically, very limited informal relations, between ECTC and some NATO bodies. Does your team maintain any contact or any working relations at all with anyone from NATO?

JS: So, in Europol, we have strategic agreements. If you go on Europol’s website, you can see the strategic agreements that we have, and one of them is with the Counter-IED COE in Madrid […] recently not so much, but we also have contacts with the COE in Slovakia, the EOD COE, and with you guys, we invite you every year to the European EOD Network [conference], a one-week conference every year.

We always invite you, [but] we don't have a written agreement. It's one of the fields that we would like to definitely improve. Of course, with EDA, the European Defence Agency, we have, but they are more European focused, so it's natural.

But with NATO, it's these three: the IED, the EOD, and the CBRN. For the first one, the IED, we have an agreement. For the other two, we don't.

MK: So, we have an EU point-of-contact here, but he has no relation with Europol, and that's been, I think, one of the goals with this project – raising awareness within the COE and the broader organisation itself of [the fact that] there's an agency out there that is very involved in this and, hopefully, outlining some ways in which cooperation could be improved moving forward.

JS: Yeah, we are more than welcome to have more civil-military cooperation. It is, actually, one of our goals in the future. Also with private entities, we believe that we should focus a bit on that.

MK: You mentioned trying to increase that civil-military cooperation. When it comes to CBRN, and the CT mission, is that primarily with other EU defence-related agencies?

JS: We have with the European Defence Agency. They have a project – PT-CIED, so Project Team Counter-IED, and they have multiple partners, we are one of them. When it comes to military, I think this is the only agency or body outside the national level because as I told you, in some countries, the national authority or the competent authority is military. So with them, we have a very close relationship, but not with the bodies or the agencies besides EDA.

MK: So, going back very briefly, I know you mentioned the ATLAS network. I know that they don't have, at least from what I've read until recently, a CBRN cell or a working group. Is that the role that you fill in your relationship with them, bringing CBRN knowledge to the network?

JS: ATLAS is also a network, and they have two members here at Europol […] however, these are special intervention units. So, their focus on CBRN is just going in, take the hostage, go out (e.g.). It's just a very brief intervention on CBRN […] we liaise with them, assist them in their trainings if they need expertise or we can, if they ask, and we do this quite often, point [someone] out to them.

So, they reach out to us, "hey, we would like an expert on chemical weapons, nerve agents". Because we have a very good mapping on the European level [regarding] capabilities and people, we can say, "OK, reach out to this guy [to see] if he can assist you in training or something like this".

But they do have a focus on CBRN, keeping in mind the overall roles or tasks that they have […] they don't collect evidence, they don't do [decontamination], they don't do reconnaissance, monitoring. They don't do anything of this. They just go in, do whatever they have to do for five minutes, and they're out.

MK: For them, it's more of an operating environment than an actual specialty to focus on. Zooming out, I'd be really interested in getting your opinion, within the bounds of classification of course, of the CBRN terrorist threat within Europe nowadays and what you think the role of ECTC and your team will be moving forward.

JS: The CBRN threat is low likelihood, high impact. We see it maintaining this, so we don't see the change. It's not that the likelihood of events or attacks have increased, but if you Google, you will see some incidents, some of them with improvised substances but some of them with actual nerve agents.

In the Czech Republic, there was a case with Sarin not so many years ago, in which Sarin was found in an old storage house. So, not to be used, but it's a reflection that this is out there. So, in this case, it was found by someone with good intentions, and they called the authorities. But this happens. There was also a case with mustard, the gas in a liquid form in Georgia, a few years ago in the airport.

So, when we put together the threat picture, we see the intention. The intention is quite high. And we see a lot of intent to [construct] a dirty bomb, not necessarily feasible, not necessarily with the best ingredients to have a successful dirty bomb. But we see this intention.

When it comes to capabilities, because the threat is a sum of capabilities and intention, we see that this is where the gap is still there. That's why the threat is a bit stable, I would say.

The biggest threats or emerging threats in my eyes is, of course, the Ukrainian conflict. I told you before, the substances that are out of regulatory control because of Zaporizhzhia, because of Chernobyl. This is one of the biggest threats that we see, I would say that [another emerging one] is related to AI and the use of LLMs as a crime facilitator or catalysts to accelerate the process of knowledge gaining. So, this is what we see as a main concern, and we are also tackling this.

MK: It's interesting that you mentioned the LLMs because I was reading something published last year from a university in the US, where a group of students managed to plan out the acquisition and weaponisation of a pathogen in about an hour using an LLM. So, it's interesting that that's something you have caught onto as well.

JS: I think it was in the beginning of this year, if you go on Open AI, you will see they did a red teaming exercise on bio. They hired 100 specialists, and then they divide the group into 50 people each, and they tried to test their system on how easily they could use open-source AI to [stage] a bioterrorism event. Because it was a test done by Open AI, the result, of course, would always be "everything is OK, no need to worry". But if you read between the lines, you will see that maybe you should be worried.

It's a challenge that we have in our hands because, as I said, the intention is very clear, but what is missing now are the capabilities, and AI is a facilitator.

MK: Yeah, it's bridging that gap in the capability.

JS: Yeah, of course it's impossible for you just to have the knowledge. You need to acquire the precursors or the chemicals, you need to synthesize, you need to buy the lab equipment, you need to find a way to weaponize it. So, there are many stages, and it takes time to perform all of the stages. However, with the LLMs, the window of opportunity for law enforcement to act is reduced. So that's why we see it as a threat, of course.

MK: So, for us, the term that they use in NATO is the "proliferation pathway", going from that intention all the way through to acquisition, developments, and eventually employing the weapon. The role that I imagine for Europol is working to interdict that by supporting the national authorities.

JS: Yep, Yep, this is exactly what we do. So, in each stage of this CBRN [or explosive] attack, we try to tackle it like this web prevention, […] but we focus only on nonstate actors. We don't focus on state actors. The only time we focus on state actors is on conflict, but [without] focusing on their intentions. So, we don't focus on Russian intentions; we focus on the devices that they use, the UAVs that they are using, [weaponizing] UAVs for explosives or CBRN as well, even though CBRN is a bit low here.

But this is the only time we focus on state actors. Just for the technical part because we know that the expertise or the knowledge from state actors [on] drone, for instance, can easily be shifted to non-state actors, and bad actors can use this knowledge that is online for everyone to see. So, this is where we're focused, but not so much on the intentions compared to you guys.