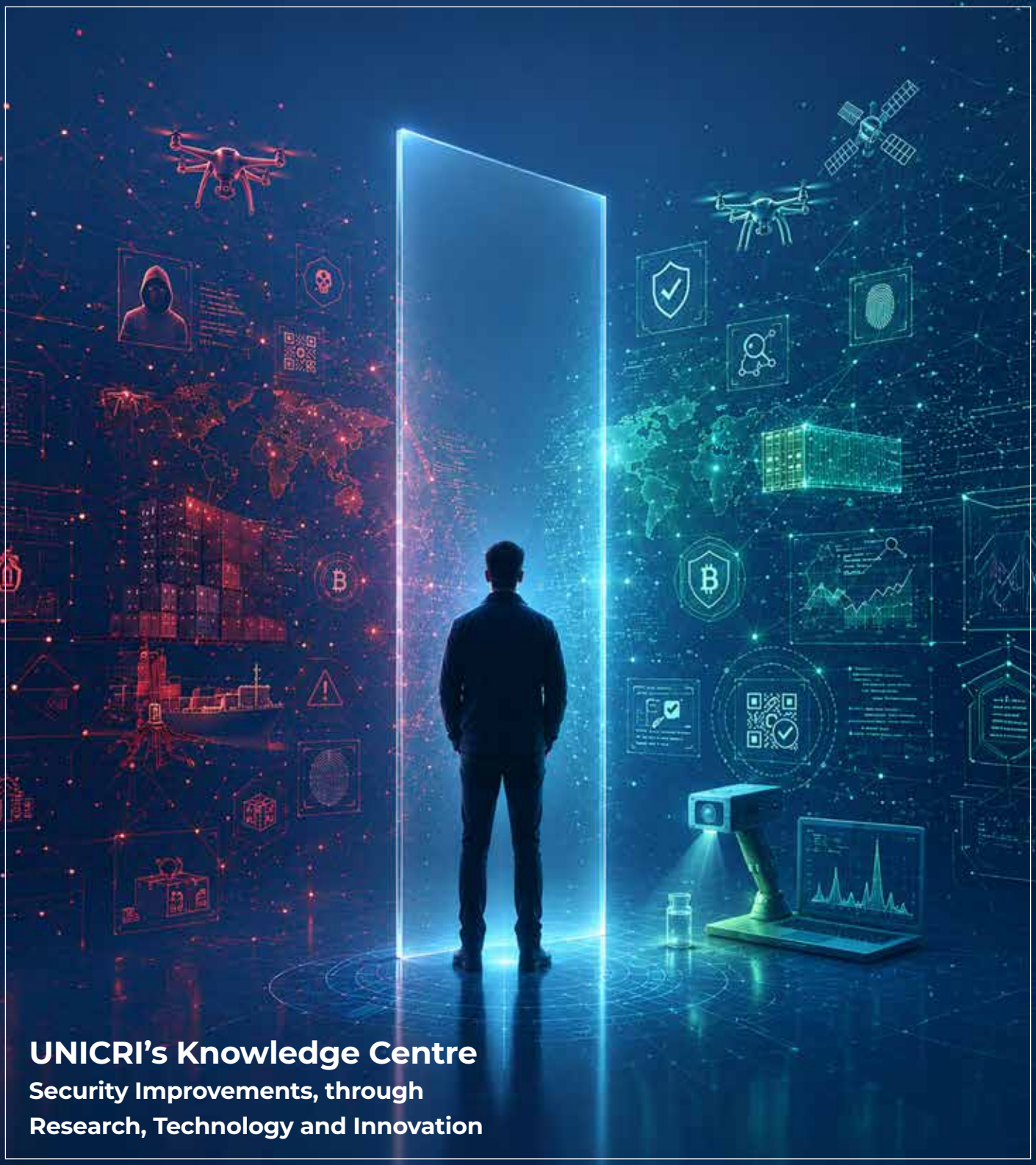
unicri
United Nations
Interregional Crime and Justice
Research Institute

10 Years of SIRIO



UNICRI's Knowledge Centre

Security Improvements, through Research, Technology and Innovation

10 Years of SIRIO

Acknowledgements

This report was written by Cristina Nastasa, UNICRI Fellow, under the supervision of Marco Musumeci, UNICRI Programme Management Officer, and Francesco Marelli, UNICRI Head of Unit, CBRN Risk Mitigation and Security Governance Programme, with editing by Marina Mazzini and design by Antonella Bologna.

Disclaimer

Copyright

Viale Maestri del Lavoro, 10, 10127 Torino – Italy

Website: www.unicri.org

Published in June 2026

Contents

UNICRI's Knowledge Centre: Security Improvements, Through Research, Technology and Innovation (SIRIO)

Using Using New and Emerging Technologies to Address Crime and Security Threats

New and emerging technologies are reshaping the criminal justice landscape – simultaneously acting as disruptors, enablers, and instruments of crime while unlocking powerful capabilities for prevention, detection, and control.

In this context, SIRIO examines a range of interconnected criminal activities, including illicit trade, organized crime infiltration into supply chains, financial crimes, technology-facilitated fraud and exploitation, and risks related to chemical, biological, radiological and nuclear (CBRN) materials and weapons of mass destruction (WMD) proliferation pathways, through which criminals increasingly leverage digital tools, datadriven logistics, and anonymization technologies to scale their operations and evade detection.

While the misuse of evolving technologies can pose significant challenges to licit economies, including the distortion of competition, the erosion of tax revenues, the undermining of consumer safety and trust, and increased compliance burdens, it can also directly affect critical security sectors such as health and pharmaceuticals, energy, transport and logistics, critical infrastructure, the financial system, and the CBRN/WMD nonproliferation ecosystem, where integrity, resilience, and effective governance are essential.

At the same time, technological innovation offers powerful instruments for law-enforcement and regulatory authorities. Advanced analytics, big data, authentication, and traceability tools can enhance monitoring, support investigations and prosecutions, disrupt criminal networks, and strengthen early-warning and deterrence capacities. As such, these tools can be effectively leveraged to identify anomalies, map risk nodes, and improve transparency across financial systems and supply chains, supporting, for example, the detection of illicit financial flows, the dismantling of networks involved in counterfeit and illicit goods, the identification of technology-facilitated exploitation, and early identification of indicators relevant to CBRN/WMD nonproliferation.

By addressing both "sides of the coin" of technology, SIRIO highlights opportunities to reinforce accountability, resilience, and integrity across critical sectors.

About SIRIO

Developed by UNICRI in 2016, SIRIO aims at increasing knowledge and information sharing on technological capabilities underpinning government security, fostering cooperation among national authorities, industry, academia, and international organizations, and actively supporting priority areas in which technology plays a key role in prevention, preparedness, and response, by matching security needs with practical technology solutions.

SIRIO's work is grounded in the reality that organized crime and non-state malicious actors continuously adapt to technological advancements in an increasingly interconnected global environment. They exploit market integration and structural vulnerabilities in globally integrated systems — particularly in supply chains, digital and financial infrastructures, and sensitive domains such as biotechnology and CBRNrelated areas — to infiltrate legitimate channels, expand illicit activities, and generate illicit profits. These dynamics have far-reaching economic, social, and political consequences, affecting the integrity of licit markets, public safety, and governance across sectors.

Recognizing that technologies can be used both to facilitate criminal activities and to support prevention and response efforts, SIRIO aims to engage various actors across different mandates and domains of expertise, with a view of reinforcing analytical capabilities and advancing joint efforts to prevent, detect, and respond to emerging vulnerabilities.

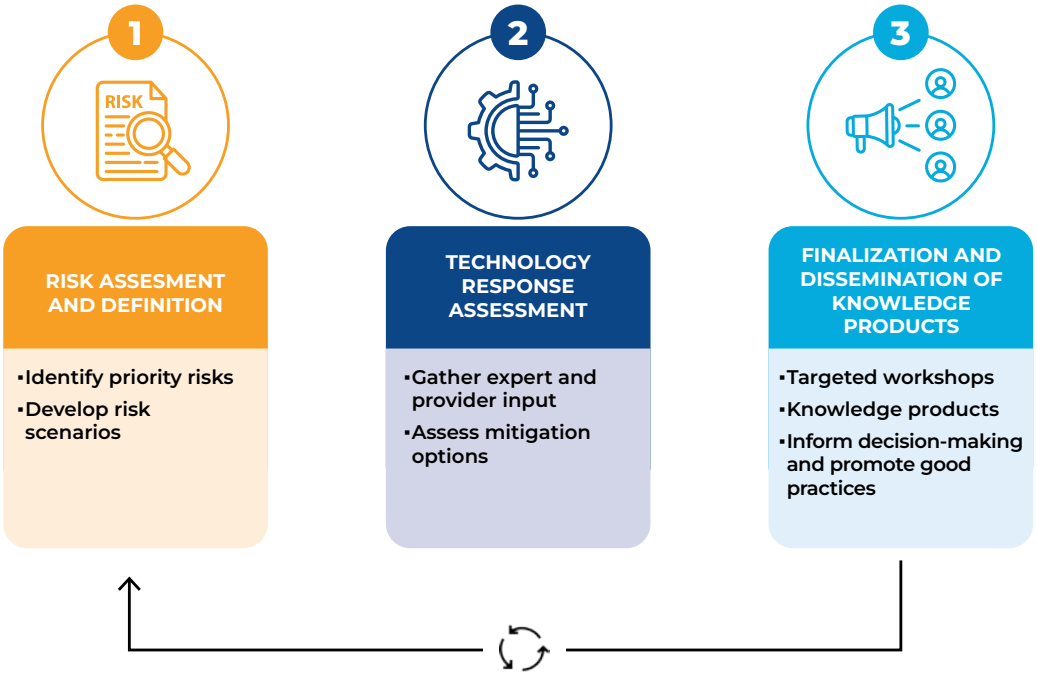
How SIRIO Works

Developed to analyze and promote knowledge and technology-based solutions aimed at addressing emerging security risks, SIRIO identifies and assesses such risks with the aim of mapping relevant technological innovations to address them, raising awareness and informing policymakers about evolving challenges and innovative responses, and enhancing cooperation among national and international authorities, industry, and research institutions.

This includes determining whether, and in what ways, the misuse of technology constitutes a security vulnerability in itself — for example through the exploitation of dual-use capabilities, the manipulation of data systems, or the subversion of critical processes — and, in parallel, identifying how technology can be used to mitigate such risks by improving the overall resilience of systems, infrastructures, and mechanisms against criminal activities.

Drawing on the feedback received in meetings and on research undertaken by UNICRI, this dual approach seeks to enhance prevention, detection, and response capacities to address multifaceted risks.

HOW SIRIO WORKS



To implement this approach, SIRIO proposes a structured, end-to-end process encompassing:

- a risk assessment and definition cycle to identify priority risks and develop concrete risk scenarios;
- a technology response assessment cycle to gather input from experts and providers on mitigation options based on the previously developed scenarios;
- dissemination of results through targeted workshops and knowledge products to inform decision-making and promote good practices across sectors.

Main Objectives

- Increase knowledge and information sharing on technological capabilities in key security areas and on how such technologies may be misused to support organized crime and terrorist activities.
- Enhance dialogue and the exchange of good practices between government representatives, technology providers, academia, research institutes, public sector representatives and industry associations.
- Match government needs with technological solutions.
- Inform policy-makers about evolving risks and effective technological responses.

Areas of Work Include but Are not Limited to:

- Supply chain security – scaled traceability, authentication, risk mitigation.
- Biotechnology and nanotechnology – dual-use safeguards, risk reduction.
- Digital forensics and cyber resilience – digital evidence, forensic analysis, threat prevention, breach protection and incident response.
- CBRN management – prevention, detection and response to CBRN emergencies.
- Organized crime and terrorism – intelligence and technology led disruptions
- Weapons of mass destruction – non-proliferation, verification and threat reduction.

Partners and Contributors

Governmental agencies – by virtue of their public mandate – play an important role, contributing throughout SIRIO's cycle, from the creation of risk scenarios to their validation, while also benefiting from the insights generated by SIRIO.

Technology providers – by participating in the call for submissions, industry representatives share innovative ideas and technical insights to address identified security gaps and challenges. They explore potential technological solutions to mitigate identified risks and, when appropriate, align, tailor, or co-develop solutions that fit countries' operational contexts, infrastructure, and governance requirements.

International organizations – bring together diverse expertise, enhancing cross-border information sharing, and ensuring broad dissemination of SIRIO outputs to inform relevant stakeholders.

Academia, industry associations and industrial stakeholders – offer different perspectives and contribute with expertise drawn from their activities, research and technical knowledge in the field.

Knowledge Products 01

Within the framework of SIRIO, three analytical reports were developed to examine the evolving intersection between technology, security and complex transnational threats. Two of these reports focus on supply-chain security, while the third addresses the topic of weapons of mass destruction (WMD). The first, Ensuring Supply Chain Security: The Role of Anti-Counterfeiting Technologies, published in 2016, provided an initial mapping of technological solutions aimed at protecting legitimate supply chains and preventing the circulation of counterfeit goods. Building on this groundwork, the second report, Technology and Security: Countering Criminal Infiltrations in the Legitimate Supply Chain, published in 2021, examined how criminal actors exploit technological, regulatory and structural vulnerabilities, and how emerging technologies can be leveraged to counter such infiltrations. The third report produced by SIRIO focused on the area of WMD and was finalized in 2021. This report analyzed the implications of scientific and technological advances for WMD-related risks, while also identifying opportunities to strengthen prevention, detection, and response through technology-enabled approaches.

When taken together, these reports reflect SIRIO's ongoing efforts to examine the role of technology in shaping contemporary security challenges and to support a deeper understanding of how innovation can inform prevention, risk mitigation and policy responses.

1.1 Supply Chain Security

1.1.1 The UNICRI Report "Ensuring Supply Chain Security: The Role of Anti-Counterfeiting Technologies"

The full version of the report can be downloaded HERE

Introduction

This report analyzes how anti-counterfeiting technologies strengthen national strategies to protect governments and citizens by ensuring that only legitimate products circulate within legitimate supply chain. It situates counterfeiting as a complex, multilevel threat – one that endangers public health (e.g., falsified medicines and foodstuffs), erodes trust, and deprives governments of revenue from excisable goods.

Objectives of the report

Being the first of a series of knowledge products produced by SIRIO, this report aimed to provide a mapping of anti-counterfeiting technologies and to examine their role in ensuring supply chain security. In particular, the report aimed to improve understanding of how technological solutions can support the protection of legitimate supply chains by enhancing traceability, authentication, and oversight mechanisms, thereby contributing to increased security, transparency, and resilience across supply chain systems.

Process

This report was developed using a mixed-methods research approach that included desk research, a survey questionnaire, and interviews with technology providers responding to UNICRI's call. Based on responses from eighteen technology providers contacted as part of a wider outreach initiative, and accounting for confidentiality-driven data variability, this study analyzes technology-driven approaches to strengthening supply chain security across multiple product categories.

Results

In addition to legal and implementation aspects, a series of case studies were examined, providing a more comprehensive overview of the technological solutions available at the time. These cases documented existing practices while also highlighting innovative applications and emerging trends, illustrating the evolving potential of anti-counterfeiting technologies to support supply chain security, as follows:

On tax stamps and product protection systems, 26 cases were examined across the following fields of application:

- Tobacco products: in Brazil, the State of California, Canada, the State of Massachusetts and the State of Michigan – information was provided by OpSec and SICPA.
- Alcoholic beverages: in Brazil, China, Delhi (India), South America and Thailand – information was provided by Advanced Track and Trace, Authentix, De La Rue and SICPA.
- Joint schemes for tobacco products and alcoholic beverages: in Georgia, Kenya, Kosovo, Kyrgyzstan, Morocco, Mozambique and Turkey – information was provided by De La Rue, OpSec and SICPA.
- Pharmaceutical products: in Malaysia and Turkey – including two examples of technological solutions applied at the national level – information was provided by Hologram Industries and Technarts.
- Multi-product protection schemes: in Albania, Armenia, Belarus and Sri Lanka – referring to cases involving the application of a single technological solution for the protection of several products in a given country simultaneously – information was provided by AM-PG Group (e.g. tobacco, alcoholic beverages, soft drinks and pharmaceutical products) and SICPA (e.g. pharmaceutical products, soft drinks, toothpaste, edible oil and electrical appliances).

- Oil and gas: in Guyana and Serbia – information was provided by Authentix.
- Textiles: identification of fibre content in premium Pima cotton garments and ensuring quality and label compliance in Pima cotton products – information was provided by ADNAS and Tracekey.

On security documents:

- Electronic passports: in France, Cameroon, Germany, the United Kingdom and Kazakhstan – information was provided by Hologram Industries, De La Rue and OVD Kinegram.
- Other identity documents: in Saudi Arabia – information was provided by Atlantic Zeiser.
- Certification of property deeds: in Benin – information was provided by Prooftag.
- Vehicle registration documents: in Ivory Coast – information was provided by Prooftag.

1.1.2 The UNICRI Report "Technology and Security: Countering Criminal Infiltrations in the Legitimate Supply Chain"

The full version of the report can be downloaded HERE

Introduction

Organized crime demonstrates a high capacity to capitalize on gaps within integrated supply chains, often infiltrating these systems to expand its activities.

To enhance knowledge in this field, UNICRI published this report to outline major supply chain threats and present technologybased responses that support legitimate stakeholders and equip law enforcement with additional tools to investigate and counter organized crime activities. The report does not position technology as the sole solution to mitigate identified risks, but rather as a means to augment human capabilities. Examples showcase different approaches that can be applied to mitigate threats through the use of artificial intelligence, big data analytics, advanced authentication and traceability systems, and nuclear analytical techniques.

Through this report, technology is presented as a key tool to support the development of new strategies, generate knowledge, and adapt responses to increase their efficiency and accuracy.

Areas Covered by the Report:

- **Agro-food mafia:** over the past few years, the involvement of organized crime groups in the agri-food sector has become more prominent and is commonly referred to as "agro-mafia". Such infiltration has serious implications for consumer health and safety and contributes to significant illicit revenues for criminal groups. Organized crime infiltrates the agro-food sector to launder money, boost profits, and control supply chains, using corruption and intimidation to undermine competition. This results in widespread food fraud, with counterfeit products which are often discovered in markets with limited oversight. Consequently, legitimate businesses suffer economic losses, enforcement is tougher, and consumers face increased health and safety risks.
- **Illicit trafficking of precious metals, including counterfeiting operations and illegal mining:** this phenomenon is connected to other forms of criminality, such as product theft and illicit financial flows. Organized crime exploits the precious metals sector through illicit trafficking, counterfeiting, and illegal mining, which harms economies and communities. These activities involve corruption, online fraud, tax evasion, and theft of valuable recyclable components such as catalytic converters, leading to environmental degradation, human rights abuses and risks to public safety and socio-economic stability.
- **Illicit, Unreported and Unregulated (IUU) fishing:** a lucrative business increasingly operated by organized criminal networks, which systematically engage in this low-risk, high-return illegal activity in a context of overfishing and diminishing stocks. Criminal networks exploit weak governance to engage in IUU fishing, misleading consumers through mislabeling, species substitution, and falsified documentation. These practices deplete fish stocks, threaten food security, and result in significant economic losses for coastal and developing communities.
- **Trafficking in counterfeit and substandard pesticides:** an activity carried out by organized criminal networks, which exploit international shipping routes to disseminate expired, counterfeit, and unauthorized pesticides. These illicit products introduce toxic substances into farms and ecosystems, threatening workers' safety and consumers' health. Their presence undermines legitimate producers, reduces agricultural productivity, and causes long-term environmental and public health issues.
- **Fuel fraud:** the fuel/oil sector is particularly vulnerable to criminal activities, which affect the entire supply chain. Organized crime exploits weaknesses across the hydrocarbons supply chain by stealing, adulterating, and smuggling fuel to evade taxes and sell it at low prices. These methods – from excise-duty fraud to chemically "cocktailing" fuels – inflict major financial losses on governments and legitimate businesses, distort market competition, undermine energy security, damage infrastructure, and strengthen criminal economies, all at a high cost to public safety and government revenues.

Objectives of the report

- Understand how technology can support efforts to mitigate threats posed by organized crime in different fields, such as counterfeiting and food fraud, Illicit, Unreported and Unregulated (IUU) fishing, the trafficking of precious metals, counterfeit and substandard pesticides, and fuel fraud.
- Analyze organized crime involvement across sectors and supply chain stages and evaluate the potential of supply chain security solutions to mitigate risks in the fields considered by the report.
- Increase knowledge and information sharing on key technology features for security in the fields covered by the report.
- Facilitate dialogue and the sharing of good practices between technology providers, representatives of the public sector and industry associations.
- Inform policymakers about identified security risks and evolving policy and technology solutions.

Process

- For each field considered in the report, UNICRI internally reviewed case studies and developed the following risk scenarios to facilitate discussion between experts:
  - Three risk scenarios on food fraud were prepared, in cooperation with the International Criminal Police Organization (INTERPOL), the European Union Agency for Law Enforcement Cooperation (Europol), the Italian Carabinieri, the German Federal Criminal Police Office (Bundeskriminalamt – BKA), and the German Federal Office of Consumer Protection and Food Safety (Bundesamt für Verbraucherschutz und Lebensmittelsicherheit – BVL):
    1. *Infiltration of the Dairy Supply Chain (milk and products made from or containing milk)*
    2. *Parallel Market for Catering Supplies*
    3. *E-commerce: Criminal Infiltration of Online Supermarket Chains for Home Delivery of Fake Food*
  - One risk scenario on IUU fishing was prepared in cooperation with INTERPOL.
    1. *Criminal Influence over Port Workforce and Contracts*
  - One risk scenario on illicit pesticides was prepared in cooperation with the Food and Agriculture Organization of the United Nations (FAO) and Croplife International.
    1. *Infiltration into the Agrochemical Supply Chain*

- Two scenarios on fuel fraud were prepared in cooperation with Pierre Viaud Consulting.
  1. *Infiltration into the Supply Chain*
  2. *Fuel Laundering and Mixing*

Innovative ideas to address counterfeiting and criminal infiltration in the supply chain Deadline: 29 February 2020

28 Nov 2019

Geneva (Palais des Nations), 28 November 2019. Preventing and combatting counterfeiting and criminal infiltration into the legal economy is very complex. Organized crime groups are showing alarming capabilities to infiltrate different sectors of the economy, including the health care sector and other public services, the construction, the transportation and logistics, the mining supply chain, the financial activities and the business of restaurants, hotels and bars. Some groups can also be very ingenious in developing strategies to conceal and launder their money and exploit all vulnerabilities of the legal economy.

UNICRI and the European Space Agency (ESA) are looking for innovative ideas and new solutions that can concretely contribute to mitigating emerging and future risks posed by counterfeiting and criminal infiltration in the supply chain.

UNICRI is interested is ideas and solutions that can address, in particular, risk scenarios in the following areas:

- Food Fraud
- Illegal, Unreported and Unregulated (IUU) Fishing
- Counterfeit and Substandard Pesticides
- Fuel Fraud

Illegal Mining and Trafficking of Precious Metals

The call is launched by UNICRI within the framework of UNICRI's SIRIO initiative in Geneva. The call is for security experts and representatives from industry, academia, civil society organizations and international organizations. The results will be used to compile a **Report on Emerging and Future Risks** that will scan the horizon of technology solutions and services to anticipate and mitigate risks posed by counterfeiting and criminal infiltration in the supply chain.

- Three scenarios on illicit trafficking in precious metals were prepared in co-operation with the International Platinum Association.
  1. *Illicit Trafficking of Precious Metal Materials*
  2. *Illicit Trafficking of Counterfeit Gold Bars*
  3. *Infiltration of the Legal Industrial Refining Process*

- The risk scenarios were discussed and validated during an ad-hoc meeting organized in Geneva, at UNICRI's Office located at the Palais des Nations.
- The validated scenarios served as a basis for the creation of a call for submissions of technology inputs. In particular, through the call UNICRI invited security experts and representatives from industry, academia, civil society and international organizations to share innovative ideas and solutions that could concretely contribute to addressing one or more risks highlighted in the prepared scenarios, which were shared with experts responding to the call.
- Responses from experts and technology providers were submitted through written contributions, outlining how existing or future technologies could respond to the challenges identified in the risk scenarios.
- Information received following the call for submissions was evaluated against the specific risk scenarios through a series of meetings involving the stakeholders who presented a submission together with the experts who cooperated with UNICRI in the development and validation of the risk scenarios. Results from these meetings allowed UNICRI to develop a preliminary overview of the technological opportunities and limitations that existed at the time.
- The information collected through the overall process was synthesized by UNICRI into the final version of the report.

Examples of risk scenarios and the evaluation of technology responses are presented in Annex 1 for the areas of illicit pesticides and fuel fraud.

Results

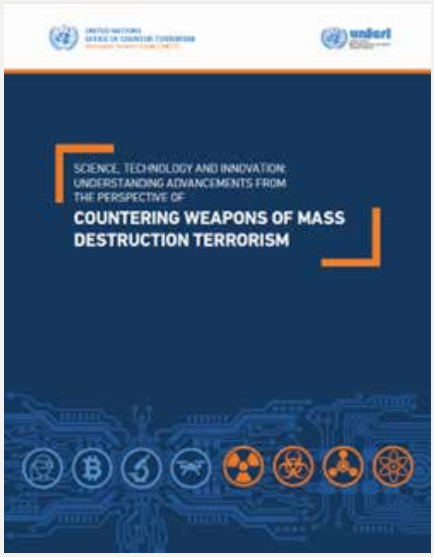
By systematically evaluating all inputs received against the specified risk scenarios, this eport presents a picture of the strengths and limitations of technologies available at the time. While no single solution can fully address the breadth of supply-chain risks, several technologies show cross-cutting relevance across sectors and functions.

When applied in combination, multilayered technological measures – such as product authentication, secure traceability, advanced analytics, and integrity-verification mechanisms – reinforce one another to significantly enhance security and reduce opportunities for malicious actors.

For each field considered by the report, SIRIO developed and disseminated an analysis illustrating how technology can strengthen Member States' security, as well as how its misuse can create vulnerabilities. The findings of this action-oriented research were subsequently translated into specialized technical workshops aimed at fostering a common, evidence-based understanding of both opportunities and risks, and supporting targeted capacity-building efforts and coordinated action against malicious threats.

1.2 Weapons of Mass Destruction and Terrorism

1.2.1 The UNICRI Report: "Countering Weapons of Mass Destruction (WMD) Terrorism"



The full version of the report can be downloaded HERE

Introduction

The report Countering Weapons of Mass Destruction (WMD) Terrorism is a SIRIO output, produced by UNICRI and the United Nations Office of Counter-Terrorism (UNOCT) within the framework of the United Nations Global Counter-Terrorism Coordination Compact Working Group on Emerging Threats and Critical Infrastructure Protection.

Objectives of the report

The objective of the report is twofold: first, to understand possible risks associated with the malicious use of science and technology to develop and deploy WMD, and second, to identify scientific and technological solutions that can be used to fulfil United Nations Member States' needs in terms of preventing and combating WMD terrorism.

Process

The process for the preparation of this report was similar to that followed in the elaboration of the report on criminal infiltrations into the legitimate supply chain, encompassing risk assessments, fictional risk scenarios based on real cases, technology response assessment cycles (including a Call for Innovative Ideas to Address WMD Terrorism), and finalization of a dedicated report.

- A series of risk scenarios were prepared on the following topics: misuse of unmanned aerial systems (drones); AI-powered cyberattacks; misuse of synthetic biology, including gene-editing technologies; and misuse of additive manufacturing.
- In particular:
  - Two risk scenarios were elaborated for the topic of misuse of unmanned aerial systems: one on a chemical attack using a drone and one on sabotage of a chemical facility carried out with a drone;
  - Two risk scenarios were elaborated for the topic of AI-powered cyberattacks: one on undermining trust in vaccines during an outbreak and one on AI-powered cyberattacks against a nuclear facility;
  - Two risk scenarios were elaborated for the topic of misuse of synthetic biology: one on agroterrorism exploiting DNA synthesis technology and one on deliberate food contamination using Clustered Regularly Interspaced Short Palindromic Repeats (CRISPR);
  - One risk scenario was elaborated for the topic of misuse of additive manufacturing focusing on the illicit trafficking of nuclear components.
- The risk scenarios were discussed and validated with experts during a dedicated meeting organized in Geneva, at UNICRI's Office located at the Palais des Nations.
- A call for submissions of technology proposals was organized by UNICRI to collect concrete ideas on technology responses to the threats identified in the risk scenarios. These proposals were reviewed and validated through three virtual expert meetings on:
  - Using Big Data Analytics and Blockchain to Combat WMD Terrorism
  - Using Virtual Reality (VR) and Drones to Combat WMD Terrorism
  - Using Biotechnology to Combat WMD Terrorism
- The information collected through this cycle of risk scenarios and related technological responses allowed UNICRI to draft the report. Given its contents, the report was initially kept confidential. However, several of the key threats and technologies included in the report are now in the public domain and the report has been made public.

Examples of risk scenarios and the evaluation of technology responses are presented in Annex 2.

Results

Although a range of structural and normative factors have historically constrained the likelihood of WMD terrorism, continued advances in science and technology have the potential to alter these dynamics. In this context, a credible risk persists of terrorist actors seeking to leverage technological progress to pursue WMD-related objectives.

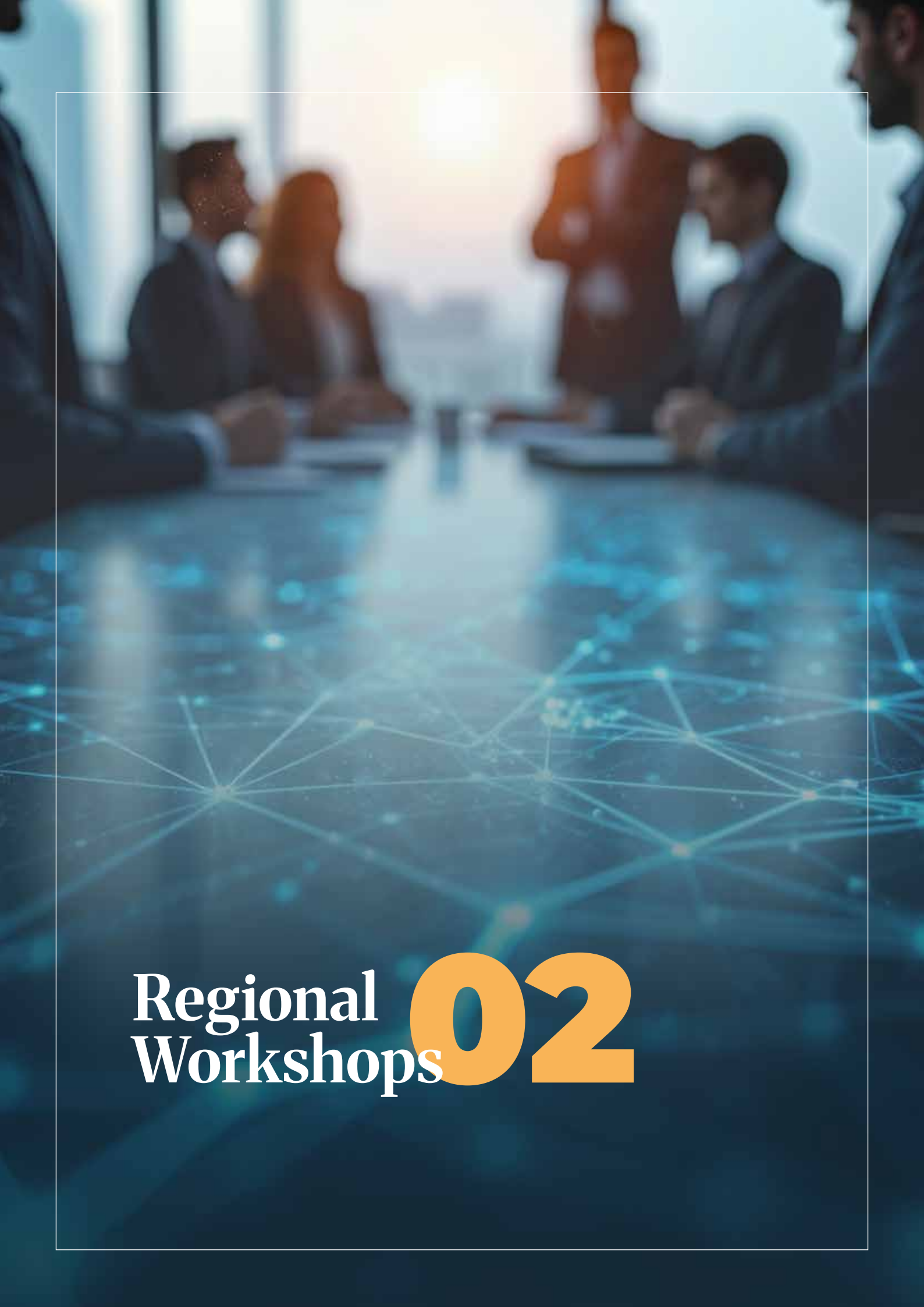
The report identifies a range of risk scenarios associated with the misuse of emerging and commercially available technologies – including the potential use of unmanned systems for the dispersal of CBRN materials, advanced computational tools to target or disrupt critical chemical or nuclear infrastructure, and additive manufacturing to support delivery capabilities. Additional risks stem from the exploitation of specialized human expertise and the combined use of technologies to enhance operational effectiveness, evade detection, and challenge existing prevention and response mechanisms.

At the same time, science and technology can play an important role in preventing, detecting, and responding to WMD terrorism. Existing technological applications – such as data analytics, blockchain-based systems, unmanned platforms, and simulation-based training – can support the protection of sensitive facilities and materials, strengthen investigative and monitoring capacities, improve early-warning mechanisms, and enhance the preparedness of frontline personnel.

The report further highlights that technology should be understood as an enabling component within broader counter-WMD frameworks, rather than as a substitute for human judgment, institutional capacity, or governance. Effective use of technological solutions depends on their integration into existing operational, legal, and organizational structures, and on the availability of skilled personnel capable of interpreting outputs and making informed decisions.

A recurring finding is that there is no universally applicable technological solution. Measures that prove effective in one operational or geographic context may present limitations or unintended consequences in others. As such, scientific and technological solutions require adaptation and customization to specific environments, risk profiles, and institutional settings.

Finally, the assessment emphasizes that technology does not constitute a definitive response to WMD terrorism. Innovation can expand available countermeasures, but it may also influence the tactics of violent nonstate actors, necessitating sustained assessment, adaptation, and coordination to ensure that technological responses remain effective over time.



Regional Workshops 02

To support the dissemination of knowledge generated through the development of dedicated knowledge products, and to facilitate structured engagement between the private sector and governmental stakeholders, a series of workshops were organized within the framework of SIRIO. These workshops served as platforms for sharing analytical findings, presenting technological developments, and fostering dialogue on emerging risks, opportunities, and good practices related to security and innovation. In addition to enhancing awareness among participating stakeholders, the workshops aimed to promote mutual understanding, encourage cross-sector collaboration, and create opportunities for sustained exchange between technology providers, policymakers, and practitioners, thereby contributing to more informed and coordinated approaches to addressing complex security challenges.

Regional Workshop

2.1 "Using Authentication Technologies and Nuclear Analytical Techniques to Counter Criminal Infiltration into the Legitimate Supply Chain"

Nairobi, Kenya, 10–12 May 2022

The workshop brought together governmental experts from the Democratic Republic of Congo, Kenya, Tanzania and Uganda, alongside representatives of INTERPOL, with the participation of the European Union Chemical, Biological, Radiological and Nuclear Centres of Excellence (EU CBRN CoE) Regional Secretariat for Eastern and Central Africa.

The event convened authorities, international organizations, law enforcement bodies and private-sector actors to address criminal infiltration in key supply chains, including fuel fraud, illicit pesticides, illegal fishing and counterfeit medicines. Participants included companies affected by these crimes and technology providers such as Authentix, Bayer, Corteva, Medisafe, SICIM and SICPA, with additional contributions from organizations attending virtually, including the International Atomic Energy Agency (IAEA), the European Union Intellectual Property Office (EUIPO) and the United Nations Office in Ukraine.

The regional meeting examined how organized crime and terrorist groups infiltrate legitimate supply chains and explored the potential of emerging technologies to reinforce supply chain integrity. Discussions focused on advanced authentication systems, traceability tools and nuclear analytical techniques for forensic investigation. Participants underscored the operational value of these technologies for national authorities and identified priorities for future action, including enhanced training, stronger inter-agency coordination and closer public-private cooperation. The event ultimately helped define concrete next steps for strengthening national and regional strategies and informing future research and technological development.

Regional Workshop

2.2 "Technology and Security: Prevention, Detection and Response to CBRN Terrorism and Organized Crime Activities"

Accra, Ghana, 27-29 March 2023

The regional meeting advanced UNICRI's efforts to strengthen responses to CBRN-related criminal and terrorist threats by bringing together national authorities, international partners and technical experts to examine how science and technology can reinforce prevention, detection and response capacities. Building on the findings of UNICRI's work on supply-chain integrity, discussions focused on the risks posed by CBRN materials and criminal infiltration into legitimate markets – including in areas such as illicit pesticides, falsified medicines, fuel fraud and IUU fishing – and on the technological solutions that can help address these threats.

Participants included national experts from Côte d'Ivoire, Ghana, Liberia, Nigeria and Sierra Leone working on CBRN risk mitigation and combating illicit trade affecting supply-chain integrity. They explored the operational value of authentication tools, monitoring and detection systems, and nuclear analytical techniques, using hands-on exercises to assess how these capabilities can support both law enforcement and scientific work. The event also gathered experts from the private sector and research laboratories, whose contributions were essential for understanding how these technologies function and the benefits they can provide. Participants included representatives from Croplife Africa Middle East, Expertise France, Focos Food, Global IPR, SICPA, the University of Cape Coast, and the University of Ghana.

The meeting further highlighted strategic needs, including improved inter-agency coordination, stronger public-private collaboration and expanded training opportunities, while confirming growing demand from participating countries for tailored national follow-up activities. Overall, the event served as an important platform for aligning regional priorities, strengthening cooperation and guiding future research and capacity-building efforts to counter CBRN-related and supply-chain-related criminal activities.

Expert Dialogue

2.3 "Technology and Security: Prevention, Detection, and Response to Chemical Terrorism and Organized Crime Activities"

Jakarta, Indonesia, 22–23 November 2023

This expert dialogue strengthened collective efforts to address chemical terrorism and the criminal misuse of hazardous materials. The event explored the evolving nexus between science, technology and security, examining risks linked to the acquisition, production and diversion of chemical substances, as well as the infiltration of these materials into legitimate supply chains. Building on UNICRI's work under the EU CBRN Centres of Excellence Initiative and on the Institute's work on technology and supply chain integrity, discussions focused on innovative solutions – including authentication systems, portable detection tools and nuclear analytical techniques – to reinforce prevention, detection and forensic capacities.

The Dialogue brought together a highly diverse group of stakeholders, including over 30 representatives from Indonesian government agencies, more than 20 participants from the private sector and research laboratories, and delegations from Cambodia, Malaysia, the Philippines and Thailand. Private sector stakeholders included representatives from Croplife Indonesia, Focos Food, Global IPR, Ineos Aromatics, SICPA, and the University of Cape Coast in Ghana. This broad participation fostered meaningful exchanges among policymakers, law enforcement officers, scientists and industry specialists, enabling a better understanding of how technology solutions function and how they can be effectively deployed. Through group exercises and casebased discussions, participants assessed the operational value of these tools and examined how they can support national authorities in monitoring, preventing and investigating chemical-related threats.

The meeting also served to identify shared strategic needs, including stronger inter-agency coordination, enhanced public-private partnerships and specialized training. By mapping existing capabilities and technological gaps related to supply chain security, portable detection tools and forensic analytical methods, the Dialogue generated a clearer understanding of the needs of participating countries and confirmed growing demand for tailored national follow-up activities.

Regional Workshop

2.4 "Combating Organized Crime and Illicit Trafficking of Critical Minerals in Southeast Asia"

Phnom Penh, Cambodia, 4–5 December 2024

Held in collaboration with the Government of Cambodia and its National Authority of Chemical Weapons (NACW), the Regional ExpertLevel Workshop examined governance challenges, supply chain vulnerabilities and organized crime's role in illegal mining and the trafficking of critical minerals, informed by preliminary findings of a UNICRI study dedicated to these issues. Designed as a regional needs assessment exercise, it explored how emerging technologies and policy interventions can strengthen national and regional responses to these challenges.

The workshop brought together 30 participants from 11 countries, including law enforcement officials, government authorities, international organizations and independent experts from Brunei Darussalam, Cambodia, Indonesia, Italy, Lao PDR, Malaysia, Myanmar, Pakistan, the Philippines, South Africa and Viet Nam. Their exchanges were enriched by contributions from the private sector (SICPA), research laboratories and organizations such as the European Space Agency (ESA), the International Criminal Police Organization (INTERPOL) and the Organisation for Economic Co-operation and Development (OECD). Working-group sessions enabled participants to analyse regulatory gaps, operational challenges and opportunities for technological support, while highlighting shared needs across the region.

Strong partnerships were central to the workshop's success. National Focal Points of the EU CBRN Centres of Excellence Initiative expressed their interest in further strengthening the regional network and in accessing additional tools and methodologies to help identify capability gaps and support the development of appropriate responses.

The Cambodian Government and NACW supported the effective implementation of the workshop where interactive exercises enabled delegations to define priority needs in legal frameworks, enforcement capacities and technology deployment.

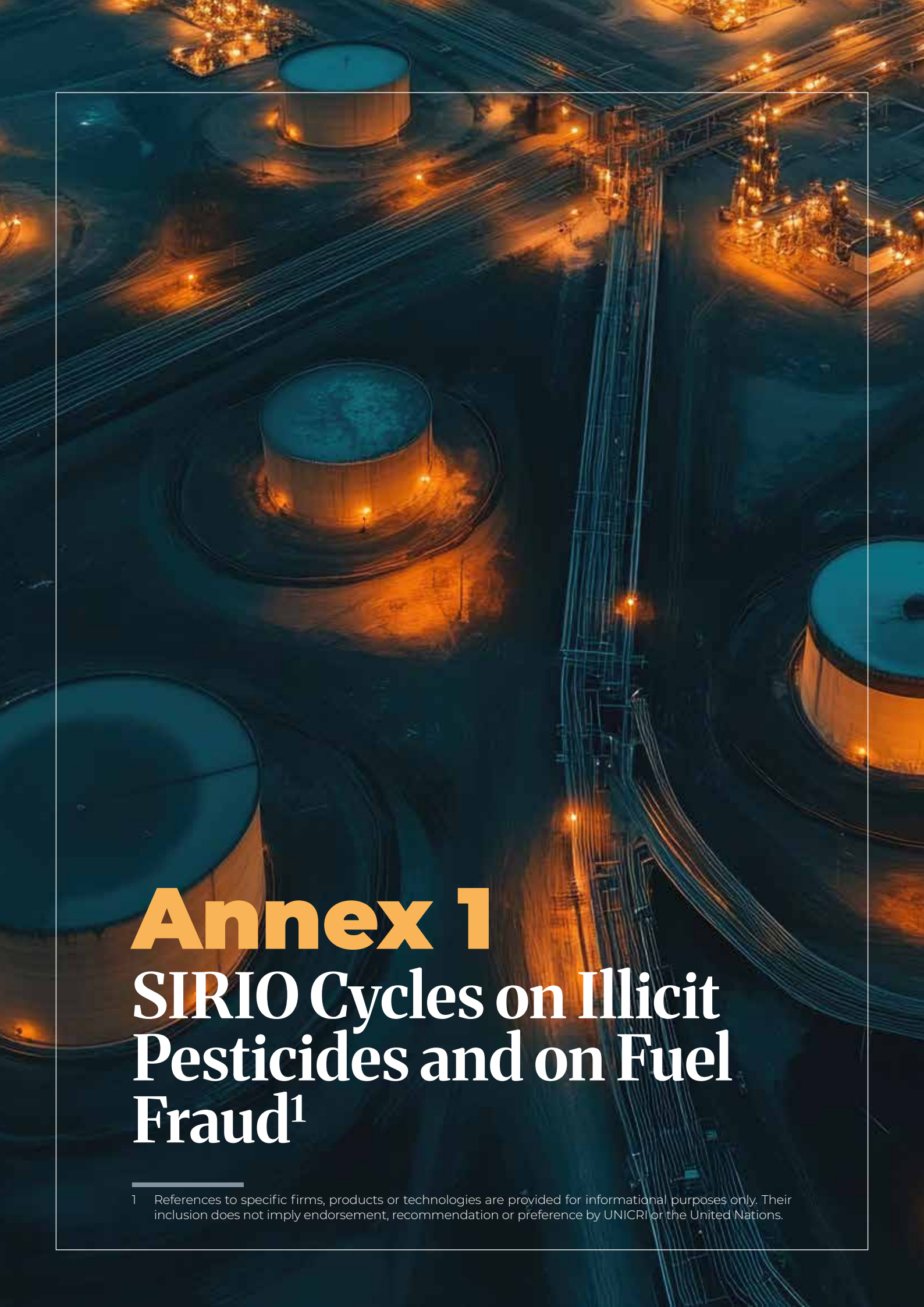
The event demonstrated strong regional commitment to strengthening supply chain security for critical minerals and generated insights that will guide UNICRI's future work in supporting efforts to counter transnational organized crime in Southeast Asia.

Way Forward

As technologies evolve rapidly, they offer significant opportunities to enhance supply chain integrity, strengthen product authentication and reduce the space for malicious infiltration across key sectors. At the same time, misuse of technology can introduce new vulnerabilities or facilitate criminal and terrorist activities, which may have serious consequences. A balanced approach is therefore needed, one that encourages innovation while maintaining safeguards so that technology consistently serves to reinforce, rather than undermine, security.

In this context, governments and technology providers at national, regional, and global levels may wish to consider cooperative measures tailored to local circumstances. These could include sustained horizon-scanning to remain abreast of emerging tools, opportunities, and risks; responsible innovation practices (including security and ethics by design, privacy and dataprotection considerations, and transparency of provenance and performance); structured information-sharing and interoperability standards among public authorities, industry, and research communities; and capacity-building to evaluate, pilot, and validate promising solutions in realistic operational settings. Attention to evidence-based policy and proportionate regulatory approaches can further align innovation with public-interest objectives while addressing the potential for misuse.

Within this framework, UNICRI, through its SIRIO programme, stands ready to support these efforts by identifying emerging and future security risks, mapping technology innovations to security needs, raising awareness, and facilitating dialogue among national and international authorities, industry, and research institutions. UNICRI will continue supporting stakeholders in strengthening the broader security architecture and in ensuring that technological progress remains a trusted instrument for enhancing CBRN management and risk mitigation as well as supply chain security and resilience.



Annex 1

SIRIO Cycles on Illicit Pesticides and on Fuel Fraud[1]

1 References to specific firms, products or technologies are provided for informational purposes only. Their inclusion does not imply endorsement, recommendation or preference by UNICRI or the United Nations.

Illicit Pesticides–Risk Scenario

Infiltration into the Agrochemicals' Supply Chain

The agricultural sector of a country is well developed but requires significant pesticides use for effective crop production. The country itself is experiencing a wave of foreign investments as a result of its recent opening up to international trade. The agrochemical industry provides a key contribution to national agricultural production. However, the legal and regulatory framework has not kept pace with the most advanced international standards on chemicals management, and the production of several highly hazardous pesticides remains legal in the country.

Always on the lookout for high profits at low risk, the ringleader of a domestic organized crime group has strong interests in the distribution of counterfeit goods, which are a low priority for national authorities and law enforcement agencies. In a bid to differentiate the group's investments, the leader of the criminal group wants to start operating in the chemical sector, especially in the pesticides area, and implements the following criminal business model:

Step 1. Acquiring control over legitimate companies: Thanks to the reinvestment of its illicit profits into the legal economy, the criminal group has taken over a chemical manufacturing plant in the country's coastal area, where major industrial development projects are taking off. The leader of the criminal group entrusts the business to frontmen with no criminal record and exploits the company's expertise and customer base to meet the growing domestic and foreign demand for plant protection products.

Step 2. Production of illicit pesticides: The criminal group takes advantage of the country's outdated agrochemicals management regulatory framework (or of the fact that the law is not enforced) to produce sub-standard products, using cheaper active ingredients and other chemicals that are not in line with the registered dossiers. These products are intended for sale in least developed countries. The criminal group also copies the container design and trademarks of well-known international companies, replacing the authentic products with low-cost and hazardous ones.

Step 3. Infiltrating the market: Unencumbered by the high research costs, associated with the development of innovative and safer active ingredients, and disregarding the potential risks related to the manufacturing and distribution of agrochemicals, the criminal group is able to offer its products at highly competitive prices, which attract the attention of hundreds of unsuspecting farmers. Some of its counterfeit pesticides are exported as ready-packed and mislabelled products. Other products are misrepresented in invoices as solvents or emulsifiers, and shipped as active ingredients or in bulk consignment, rather than as packaged goods, significantly reducing the risk of detection by law enforcement authorities.

In the space of a year, the criminal group has been able to place 1,000 tonnes of counterfeit and substandard pesticides on the market, reaping over EUR 5 million in illicit profits. The criminal group has thus infringed the intellectual property rights of major legitimate agrochemical producers, while disrupting fair competition and reducing fiscal revenues. In the same period, the sale of banned substandard pesticides has had devastating consequences in the targeted least developed countries, where leakages and the inadequate storage and disposal of toxic ingredients have contaminated livestock, waterways and the wider food chain. Tonnes of crops have wasted away on the sprayed land and soil fertility will not be restored for more than three years.

Illicit Pesticides: Technology Submissions Relevant for the Risk Scenario and Their Potential Application

This section of the Annex summarizes technology submissions received by UNICRI. A more detailed description of each technology is presented in the report, including additional information, graphics, pictures and explanatory tables.

Technology Submission 1, by Singapore Synchrotron Light Source

This submission is based on the analysis of the chemical composition of the product and proposes several solutions to detect anomalies.

These solutions use several techniques, such as:

1. The Fourier Transform Infrared (FTIR) spectroscopy measures the fundamental vibrations of covalently bound atoms in molecules and identifies the unique spectrum of a compound. It may be treated as a molecular fingerprint. An Attenuated Total Reflection (ATR) accessory is a tool used when the sample is neither transparent nor reflective for Infrared (IR). When there is intimate contact between the sample and the ATR crystal and the conditions for refractive indices and incident angle are met, the sample absorbs internally reflected electromagnetic radiation through the interaction with the evanescent wave.
2. The Optical-Photothermal Infrared (O-PTIR) spectroscopy works as a non-contact, far-field reflection mode and delivers high-quality spatially resolved FTIR transmission-like spectra below the diffraction limit of infrared wavelengths. The IR diffraction limit is overcome by combining a pulsed tunable laser with a proprietary optical technique measuring the photothermal response of the sample in a fast, easy-to-use manner. Both technologies may be applied to verify the content of the pesticides and to detect

dilution or inadequate additives. FTIR spectra may be shared among supply chain stakeholders, from manufacturers and distributors to end users, in order to check the authenticity of agrochemicals. By using semi-portable devices, it is possible to set up intermediate checkpoints to prevent the introduction of illicit products within the supply chain.

Applicability to Limit Risks Included in the Scenario

Scenario	Applicability of the solution
Scenario 1: *Infiltration into the agrochemicals' supply chain*	
Step 1 – Acquiring control over legitimate companies.	
Step 2 – Production of illicit pesticides.	The technology can be used to analyze the marketed products and determine whether they are fraudulent, of low quality, or otherwise abnormal in their composition.
Step 3 – Infiltrating the market.	The technology can be used to analyze the products placed on the market and determine whether they are fraudulent or contain sub-standard components.

Technology Submission 2, by SICPA

This submission incorporates several security layers for the creation of the digital identity of the product and for controlling its movements along the supply chain. The overall process can be divided into different stages:

1. Creating a unique identity of the product using its chemical properties and initiating physical traceability,
2. Transferring the identity into a secure database (digital identity) and initiating digital traceability,
3. Monitoring the life of the product along the supply chain and
4. Providing data analytics.

The starting point of this technology commences with the linking of the physical journey of a product to its digital journey, to guarantee integrity and auditability and to prevent fraud or diversion. This submission proposes initiating physical traceability by recording the chemical properties of the product. This initial identification is essential, as it captures and records the fundamental characteristics of the product.

This element provides a unique and innovative identification of the product at its very first point of authentication, creating its unique chemical signature. This first signature capture identifies and contains the chemical components of the

product and is further enriched with secure marking (active or passive) of the packaging. This marking also includes the signature of the product, which provides its description and credentials, including its components.

The information allows for the creation and management of "physical reference" databases, which are integral parts of this proposed solution. These databases are used to secure the aforementioned complex identity. The data is then inserted into immutable digital storage. This is a crucial step since the signature information of the product then has to be connected to a platform of integrity that will enable tracking throughout the supply chain.

To begin the digital traceability, the product identity is stored in an immutable manner using blockchain technology to achieve controlled monitoring of the various processes along the supply chain. Product packages will also be marked using information on the signature identity of the product. Where possible, in-product marking can be used. The product signature can be checked at any point of the chain with specific tools when needed.

In this regard, it has to be noted that the company developed its own tools to perform rapid signature field testing, making it possible to verify that the chemical composition of the product matches the recorded signature. For this purpose, the company developed a Portable Authentication Device (PAD) encompassing a Fourier Transform Near-Infrared (FT-NIR) spectrometer. Spectrometers are used to identify and characterize chemicals and compounds in a test sample. These devices are based on the characteristic absorption spectra determined by the chemical bonds in organic materials, which can be used to identify organic compounds, in the same way that fingerprints are used for identification. FT-NIR provides a useful complement to, or replacement for, screening methods before laborious chemistry tests and chromatographic methods. FT-NIR is non-destructive, requires little or no sample preparation, and is fast, safe and dependable, as it doesn't need dangerous chemicals.

The PAD SICPA FT-NIR spectrometer can be used on site at import points or points of sale to detect non-compliant pesticide products. The PAD in its present form cannot determine whether the deviation from the genuine signature is due to counterfeiting, adulteration, or a quality-related problem. However, coupled with the rest of the technology included in this submission, it complements the proposed approach. This gives field inspectors a useful screening tool to rapidly check whether the information included in the identification and traceability code matches the detected spectral signature without the need to perform laboratory testing.

Storage in a blockchain ensures immutability and auditability. Data is used to control processes and perform mass balance calculations to detect fraud, diversion and malfunctions during the movements of the product along the supply

chain. This feature compares data related to the volume of traded goods at their point of origin with the volume of the same goods at their point of destination. Variations in volume that cannot be justified by possible losses occurring in the normal course of trade will trigger an alarm and can represent signals of smuggling, diversion or counterfeiting operations. Data analytics and artificial intelligence algorithms provide additional means of predicting and checking the overall balance along the supply chain.

This submission also links product identification and traceability with space technologies to improve supply chain control. The idea is to use them for proof of origin as well as for track and trace, by generating data that, when combined with data obtained directly from the products, can provide a higher level of assurance regarding product quality and the integrity of transactions along the supply chain. Furthermore, satellite integration can also be used to improve the aforementioned mass balance calculations and reconciliations of trade volumes.

In particular, this submission foresees three main applications for space technologies:

1. Use for proof of origin and mass balance verification: images from drones and satellites can be used to link products to their place of origin. They make it possible to calculate production volumes and to anticipate and facilitate reconciliation.
2. Use for ensuring product quality: product quality can be assessed using specific imaging technologies, including hyperspectral cameras, to verify the origin and composition of products.
3. Use for monitoring and communication: spatial monitoring of land can also be used to detect criminal operations. Together with proof of origin, it can provide additional data to check mass balance along the supply chain.

This submission stresses the fact that secure communication and data exchanges between drones, satellites and ground-based IoTs devices are key for supply chain auditability. Therefore, it is also important to secure images, transmissions and the positioning systems of devices (IoTs and software).

Space data can be used for continuous and additional controls along the supply chain and, consequently, data and processes will also be certified and timestamped in a blockchain to improve security and avoid falsification. According to the submission, in the near future, compressed spatial images with their embedded unforgeable signatures and localizations through quantum-derived technologies will be used for this purpose. By using space technologies, the quality of the product can be assessed through specific imaging technologies, including hyperspectral cameras.

Applicability to Limit Risks Included in the Scenario

Scenario	Applicability of the solution
Scenario 1: *Infiltration into the agrochemicals' supply chain*	
Step 1 – Acquiring control over legitimate companies.	
Step 2 – Production of illicit pesticides.	This submission adds layers of security compared with more traditional approaches, such as: 1) the use of chemical fingerprinting to create the identity of the product and monitor it along the supply chain, 2) field identification through the FT-NIR spectrometer, 3) data analysis of flow mass balance of products, supported by blockchain technology and 4) the use of space technologies to add additional time-stamped controls on the origin and quality of products and their components, as well as to support the mass-balance calculations.
Step 3 – Infiltrating the market.	As previously described, the technology solution can protect the supply chain from the infiltration of counterfeit products. However, the solution would mitigate the risk only if the illicit products are introduced into the legitimate supply chain, where they can be identified through the described control mechanism.

Technology Submission 3, by Nano4u

This submission focuses on multi-layer security linked to the use of blockchain. The proposed technology solution comprises a blockchain with a bridge-database, combined with accurate time and position data from satellite navigation, and an option to digitally encrypt data from a product-level signature at origin to verify against printed packaging codes, using cryptographic keys. The blockchain can be public or private, or a combination of both, depending on the user groups involved. A trusted computing platform is used to securely interface with the internal systems of manufacturers. The different processes offered by this technology solution can be divided into:

1. Product fingerprint: The unique identification of the product (characteristics or chemical fingerprint) is obtained and linked to the traceability system. It can be read by using a smartphone or through a fast micro-level-3D scan if the digital fingerprint is on the product. Currently, the use of a chemical fingerprint is a proposal that can be adopted in this technology option if a partnership is created with other providers that have developed the technology or if it is later developed by the company.

2. Primary packaging: The initial digital fingerprint is linked to the primary packaging using cryptography to create a code. This code is verifiable by scanning it with a smartphone. An interesting feature developed by this submission is the possibility of embedding the code directly into the primary packaging so as to avoid any possibility of removing it. The company has already developed this technology and applied it in different markets.
3. Further packaging: If the product needs further packaging, the process can be repeated. The code on the new package is linked to the other codes, starting with the product-linked code. All barcodes are uploaded to the blockchain.
4. Blockchain tracking: Blockchain is used to protect the product fingerprint and the rest of the cryptographically secured codes that were used for packaging. The data is logged in a "bridge-database" between the data collection system and the blockchain. This enables visibility into changes of ownership, aggregation and disaggregation from the product-level encoding.
5. Integration with space technology: The submission also proposes integration with satellite technology to verify the origin and movement of goods along the supply chain. Verification of product flow quantities is also realized thanks to the use of both satellite integration and progressive timestamps recorded on the blockchain.

Changes in ownership of the product and aggregation and de-aggregation of containers in larger shipments are recorded immutably in the blockchain. Cryptographic keys are exchanged, allowing the receiver to become the new owner of each item when authorized to do so by the sender. Each transaction is recorded as a new block. The scanned barcodes include location and time stamping, which allows tracking of the location of the product at each change of ownership or transaction point. The scanned data is logged in a "bridge-database" as it is collected – before the hashed transaction data is saved on the blockchain. This allows data to be stored for later reference and easy verification, but groups of data are uploaded in a "hashed" form to the blockchain so that no changes to the data can be made.

An additional function uses a balance ratio between inputs and outputs that is recorded on the blockchain. For example, if the amount of pesticide and containers coming in is monitored (supported by geographical satellite data), it should correspond to a particular amount of packaged pesticide output. If the same output is achieved with a lower volume of authorized inputs, this may indicate an issue. This would require legitimate suppliers to log their shipments on the blockchain.

Sharing of relevant data is facilitated by search functions available in the bridge-database. Only authorized users have access to data. If anyone breaks into the database, no data can be changed, because it would change the blockchain. Such a change can be flagged in different ways depending on security needs, as it may not be desirable to alert everyone in the chain when such an issue occurs.

To transfer ownership of the product to the next supply chain point or end user, the sender must have both an authorized relationship with the next owner (via exchange of cryptographic keys) and a correct barcode to scan, which is traceable through the bridge-database linked to the immutable blockchain. Hence, fake containers with fake or copied barcodes cannot be used.

The recorded product and time/location data is stored for easy data access in the bridge-database but cannot be altered in any way. This allows location tracking at every uploaded data point. As a result, the history of product movement can be tracked. Regarding the security of the database, only authorized users have access to it and any change to the data can be flagged in different ways depending on security needs.

In the case of pesticide trafficking, some relevant points should be highlighted:

1. Changes of ownership in the product and aggregation/de-aggregation of containers in shipments are immutably recorded.
2. Scanned barcodes include location and time stamping (via satellite), allowing tracking at each transaction point.
3. Input-output balance ratios can be helpful in identifying an infiltration.
4. Hash-trees perfectly protect levels of information access.
5. Search functions and controlled flagging of issues.
6. Trusted computing platforms for supplier data integration.

Applicability to Limit Risks Included in the Scenario

Scenario	Applicability of the solution
Scenario 1: *Illicit infiltration into the agrochemicals' supply chain*	
Step 1 – Acquiring control over legitimate companies.	
Step 2 – Production of illicit pesticides.	This risk could be highly mitigated by the development or integration of an option using the chemical properties of the product in the code that is linked to the traceability system. Furthermore, the described use of space technology and of submission and of input-output product calculations at all nodes could be a useful element in mitigating this risk.
Step 3 – Infiltrating the market.	Risk is reduced thanks to the use of non-replicable codes that are recognizable both visually and via the use of specific tools, and by using a track and trace system and blockchain technology to secure the supply chain. The identity of each product is created by using a unique non-removable code. In this case, if the optional component is developed or integrated, the code would also include encrypted information about the characteristics of the specific product, generating a unique identification that is linked to the blockchain-protected traceability system. If an infiltration attempt occurs, alerts due to the changes in volume would be triggered. In addition, the counterfeit products would not be scannable.

Technology Submission 4, by Scantrust

The submission proposes a technology solution that focuses on applying a secure, serialized QR code in which a copy detection pattern, or secure graphic, is integrated to authenticate the product. This option enables a simple integration of the solution into the existing packaging production, which can be used by all parties across the supply chain, and is able to capture key events in the supply chain (movement of goods, transfer of ownership, among others) while being verifiable with a smartphone. The secure, serialized QR codes are managed by a connected product cloud platform. This enables several features, allowing alerts, messaging, authenticity and verification functions in one format. In addition, printing or copying the copy detection pattern in the QR code causes an irreversible information loss, which ensures that counterfeits are detected when the product is scanned with a smartphone.

The serialization of the QR codes included in the system gives any product, object, or sample a unique digital identity, and specific supply chain data can be associated with it at a unit level. The high number of scans in turn provides increased visibility on product flow in different markets and can support the early detection of counterfeit hotspots. Alerts can also be set for markers and areas identified as being at increased risk of counterfeit activity. The integration of loyalty programmes through the scanning of the codes serves as an additional incentive for customers to use the technology as often as possible.

With regard to data aggregation and binding, typically different labels are used to associate unique codes with products, cases, pallets and shipping containers. This binding makes it possible to track products geographically and activate functions such as off-market alerts, black-listing, or target-specific messaging for consumer engagement. The solution is connected to a Business Intelligence (BI) dashboard to obtain insights and predictive analytics about the products in the supply chain, which serves as a real-time tool for managing and analysing data generated in the system by scans. The codes are designed to be easily scanned and authenticated using a smartphone camera.

Digital files of secure QR codes are provided to the printer by the manufacturer. Consequently, the system could be applied to cases concerning, for example, a criminal organization attempting to take a high-resolution scan of the packaging and QR code to print it on the counterfeit product packaging. In this case, in fact, the app would generate a “counterfeit” alert if this code is scanned, due to the natural differences created by re-printing the secure graphic.

In the case in which a counterfeit code is scanned, the solution:

1. Sends an email and alert to a messaging app.
2. Reviews the scan to confirm the issue.
3. Blacklists confirmed counterfeit codes.
4. Performs deeper analysis, considering scan location, user app ID, and other scans from the same code to gain insights about counterfeit operations.

In this way, counterfeits can be identified and blacklisted before they hit the market when counterfeiters attempt to "test" their copies by scanning them. Additional features can be added to increase security, for example, a Hyperledger Sawtooth blockchain integrated into the track and trace system. The codes containing unique information about the product, as well as supply chain traceability events, are added as transactions to the blockchain, providing other characteristics such as immutability, transparency and accountability in the exchange and management of data in the supply chain.

Applicability to Limit Risks Included in the Scenario

Scenario	Applicability of the solution
Scenario 1: *Illicit infiltration into the agrochemicals' supply chain*	
Step 1 – Acquiring control over legitimate companies.	
Step 2 – Production of illicit pesticides.	The use of a unique QR code on the package of the pesticide and the use of a blockchain-protected traceability system can prevent illicit production activities involving the replication of original authentication and track and trace codes.
Step 3 – Infiltrating the market.	The adoption of this technology solution can mitigate the risk of counterfeit pesticide infiltration in the supply chain. The secure QR serialized code that is combined with a secure graphic to authenticate the product and the use of a blockchain-protected traceability system provide a solution that combines several layers of security. If the code is scanned with a smartphone, the app would detect that the pesticide is counterfeit.

Technology Submission 5, by Securikett

The submission proposes a technology solution that combines tamper protection and authentication features with a traceability system to link a unique code to a specific product throughout the supply chain. Blockchain technology is used to secure authentication data, such as product information and tracking data from tampering-related transactions. Blockchain technology can be seen as a digital tamper evidence. Data associated with the unique product identifiers (IDs) are secured by a network of decentralized nodes. Currently, this technology is considered to be counterfeit-proof. Data analytics provide insights regarding the flow of goods and supply chain infringements .

This submission emphasizes that, to protect a product on a physical level, effective tamper protection is one of the core challenges. This is valid, for instance, when using a variable code on the packaging to enable verification of the product: without appropriate tamper protection, the code can easily be transferred to a counterfeit product, compromising the effectiveness of the verification system. Security seals allow end users to check if a product has been tampered with. By using a VOID effect, a previously invisible symbol or text appears irreversibly when the seal is removed, making the latter non-reusable and non-transferrable. The patterns displayed by the VOID effect can be fully customized, using for example a lock symbol or language, in line with the security sealing label design and shape. These seals can be in different colors and shapes and can be highly translucent to leave text and barcodes underneath readable.

Security seals, including a VOID effect, allow end consumers to identify if a packaging has been tampered with. In the case of plastic screw caps, the possibility to use a seal on them is challenging, considering their small contact area to apply a seal. A dry-peel VOID, as a 2-layer construction for plastic screw caps, has been used in the pesticides market for many years. If a cap is unscrewed, the jagged design of the perforation points out that the product has been opened. Further integration of codes and security print makes the product even more secure against counterfeiting and allows all stakeholders within the supply chain to authenticate the product.

In the case of labels, they have a 2-layer construction and when a label is tampered with by peeling, a VOID effect appears. When an attempt is made to remove the label, a VOID effect is triggered between the two layers. The bottom layer of the label remains on the returnable packaging. If criminals try to reverse the manipulation attempt, the end consumer can see this through the VOID effect, as well as from the triggered perforation.

In addition to the physical product security, a security seal can be equipped with a serialized ID and a related traceability function. That means that each label has its own ID and can be managed and tracked individually. The technology proposed to enable this feature includes functions such as issuing secure codes, online authentication of each code, personalization at item level, creating response pages driven by algorithms, geotracking with full track and trace for the entire supply chain and global distribution chain, packaging aggregation management, and consumer engagement. IDs are often printed in the form of QR codes since consumers are used to scanning QR codes. Scanning such a QR code with a generic barcode reader app will lead to an authentication of the packaging and a tailored landing page showing the digital twin of this code/package/product. Individual and dynamic content is created by algorithms in view of also avoiding any tampering with the digital response. Every package and every delivery can be monitored in real-time throughout the supply chain. In addition, comprehensive data analysis helps to understand the flow of goods and possible infringements within the supply chain.

The technology submission can also be used with Radio Frequency Identification (RFID) and Near Field Communication (NFC) technology, which is based on smart labels, consisting of physical tamper evidence (VOID), the same unique ID for printed codes and the programming of individual chip content for improved product security. Depending on the product and packaging, a digital tamper evidence feature can be added to the smart labels: a built-in tamper loop indicates the opening of a product (can, bottle, case, box). A comprehensive option in the case of labels is the All-in-One label, consisting of a secure ID, RFID (NFC) and RFID and Ultra-High Frequency (UHF), all in one. The same ID is used for the printed code, the NFC chip and the UHF chip to provide full traceability throughout the entire supply chain, up to the consumer.

Applicability to Limit Risks Included in the Scenario

Scenario	Applicability of the solution
Scenario 1: *Illicit infiltration into the agrochemicals' supply chain*	
Step 1 – Acquiring control over legitimate companies.	
Step 2 – Production of illicit pesticides.	The solution is designed to mitigate the risks of a possible infiltration into the legitimate supply chain; however, counterfeit pesticides cannot be identified by their composition and the technology comes into play at the first packaging point. The technology submission provides options to authenticate the package of original pesticides by using different labels, tags and VOID effects and a secure traceability system to protect the transactions occurring throughout the product life cycle in the supply chain.
Step 3 – Infiltrating the market.	If the technology solution is implemented, the risks related to the infiltration of counterfeit pesticides can be mitigated. The use of a unique identification code that is tamper-proof and its connection to a blockchain-protected traceability system provide a multi-layered security mechanism that would detect the infiltration of counterfeit products that do not have the authentication features. The information transactions related to the movement of products through different stages of the supply chain would be immutable since they would be recorded on the blockchain.

Fuel Fraud–Risk Scenarios

Risk Scenario 1: Infiltration into the Supply Chain

Two decades ago, vast oil reserves were discovered in a given country. They were estimated to account for around 5% of the known oil reserves worldwide. A secessionist political movement is gaining increasing consensus in the area where the reserves are located, aiming to make the area independent from the national government and to ensure that revenues from oil extraction benefit only the residents of that area.

From the geographical point of view, the country shares one of its borders with another country which, in turn shares a border with a customs union (free trade area) composed of 10 Member States. The customs union has set up a computerized system for monitoring the movement of excise goods under duty suspension within the territory of its Member States. It records, in real-time, the movement of alcohol, tobacco and energy products for which excise duties have yet to be paid. It is a crucial tool for information exchange and cooperation between the Member States of the customs union.

A transnational criminal organization, the "Black Gold Ring" (BGR), aims to take advantage of any fraud opportunity that arises in the domain of oil theft and refined fuel adulteration. In order to profit from the current business opportunities of the newly discovered oil reserves, it implements the following criminal business plan:

Step 1. Political and economic infiltration: the "Black Gold Ring" secretly infiltrates the secessionist movement operating in the area and corrupts key players in the oil business (from parastatals to multinational corporations and even ship captains) in an effort to steal oil while it is being loaded from bunkering facilities onto ships.

Step 2. Infiltration into the legitimate supply chain: The head of the criminal group organizes the infiltration of stolen crude oil into the legitimate supply with the assistance of an oil trading company operating an offshore block in the neighboring country. The company artificially inflates the production volumes reported for the offshore block, thereby concealing the introduction of stolen oil transported by tanker from the neighboring country. The laundered production is then sold on to refineries established in the territory of the neighboring country. The criminal group is consequently able to collect profits from this sale and distribute these profits to the chain of intermediaries who made the first part of the deal possible. It is necessary to use a number of operations and transactions to bring the illicit

crude oil into the legitimate market in order to avoid triggering the suspicion of the public authorities. The criminal group relies on a series of mechanisms, ranging from opaque trading using ghost companies, to false documentation and invoicing, off-the-books transactions, tax evasion and money laundering.

Step 3. Infiltrating/controlling refineries: The criminal group infiltrates one of the refineries in the territory of the neighboring country. As a result, it sells regular fuel as well as cheap fuel as part of its production, with the aim of selling it in the illicit market of the neighboring customs union. Any discrepancy in price between neighboring countries serves as an invitation to smuggling operations, so cross-border crime is a recurring theme.

Step 4. Organizing a "cheap fuel trade": The criminal group organizes an illegal trade in cheap fuel, which has the potential to cause damage to vehicle engines – as the product is not compliant with the relevant customs union's standards. The cheap fuel also poses a risk to consumer health and safety due to excessive emissions. To avoid the fuel being subject to excise regimes once on the market (to avoid paying VAT or excise duty), the criminals produce a mixture composed mainly of gasoil and other added compounds to modify the final physical features of the product. As a result, the final product, which is sold illegally on the black market, is particularly attractive as it is sold at a lower price than the authentic product and enables the criminals to make huge profits. The criminal group also exploits the illegal unloading facilities and supply chains already used for other products (base oils, additives, etc.) handled by the infiltrated refinery in the neighboring country.

Step 5. Infiltration into public procurement: The criminal group undertakes another fraud scheme. The country where the reserves were discovered does not have refineries on its soil and subsidizes import of refined fuel. The head of the criminal group wants to take advantage of this situation and organizes the infiltration of the public procurement process for imported refined fuel. Thanks to corrupt government officials, he uses fuel deriving from refineries that he had infiltrated in the neighboring country and sells it, sharing the misappropriation of the granted subsidies with his accomplices.

Risk Scenario 2: Fuel Laundering and Mixing

A country is engaged in large-scale oil exploration activities off their national coastlines. The country applies a low excise rate on fuel products and has a "no-excise" policy on fuel intended for agricultural and urban development purposes, which is marked with chemical dyes. However, corruption is rampant and turning a blind eye to economic crimes in exchange for a bribe is a widespread practice.

A neighboring country, on the other hand, is led by a climate-conscious government, committed to a transition to sustainable energy sources. To that end, the government has increased excise duties on road fuel, creating a substantial price difference between the two countries. The move has resulted in higher costs for domestic industries and households, prompting discontent over its negative consequences for industry and consumers. Many motorists living in border areas have already started to refuel their tanks where it is cheaper.

Always on the lookout for high profits at a low risk, the ringleader of a criminal group in the country where large-scale oil exploration activities are taking place understands the potential high profits generated from black market sales of oil products. Anticipating a growing demand from the neighboring country due to its environmental policies, the ringleader starts operating in the fuel sector, and implements the following criminal plan:

Step 1. Smuggling: The criminal group bribes truck drivers working at State refineries to bring out fuel in small tankers. The criminal group then relies on lorry drivers and the owners of fishing vessels, interested in earning extra money, to smuggle fuel for illicit sale into the neighboring country by land and sea.

Step 2. Fuel laundering: At the same time, the head of the criminal group sets up makeshift fuel laundering plants in several warehouses of the front businesses run by the criminal group. Posing as managers of construction and agro-food companies, the ringleader's associates bribe representatives responsible for awarding licenses to participate in the national scheme for the supply of excise-free fuel. At this stage, criminals perform a chemical treatment on the rebated fuel to remove dyes and covert markers and give it the appearance of legitimate road fuel.

Step 3. Mixing and distribution of adulterated fuel: In the same facilities, the associates of the criminal group use kerosene and lubricant oils to 'extend' the diesel used as road fuel. They also add methanol to petrol for similar effect. To ensure full control of the distribution chain and maximize illicit profits, the criminal group threatens several owners of fuel pumps located in border areas to sell their business to its strawmen, who then supply adulterated fuel to thousands of unsuspecting customers from both countries.

In the space of a year, the criminal group has smuggled over 2,000,000 litres of petrol and gasoil into the neighboring country by land and sea. As both road fuels sell for EUR 1.5 per litre, the criminal group stands to gain over EUR 3 million. In the same period, the fuel laundering plants treated and passed off 1,000,000 litres of rebated gasoil as road fuel. As the country applies a EUR 0.25 exercise duty per litre of petrol and gasoil, the criminal group has carried out an excise fraud valued at EUR 250,000. Such fuel, conveyed to the stations controlled by the criminal group, was sold to domestic and foreign motorists for E 1 per litre, reaping EUR 1 million in illicit profits. The criminal group has thus caused a drop in fiscal revenues, in both countries, and has obtained a new channel for funding its illicit activities. Furthermore, the adulterated fuel damaged hundreds of car engines, and the industrial waste generated by the laundering process was illicitly disposed of in the country's river basins, resulting in serious environmental degradation.

Fuel Fraud: Technology Submissions Relevant for the Risk Scenarios and Their Potential Application

This section of the Annex summarizes technology submissions received by UNICRI. A more detailed description of each technology is presented in the report, including additional information, graphics, images and explanatory tables.

Technology Submission 1, by Authentix

This submission aims at enabling regulators to monitor and enforce key quality measures in the downstream refined fuels industry, thus preventing illegal practices such as adulteration, tax evasion (including the diversion of untaxed transit fuels into the local market), and unfair trading practices, while ensuring the delivery of high-quality fuel products to all consumers. The use of markers is an integral component of this solution, since it also enables stakeholders to combat adulteration, dilution and smuggling in gas, diesel, crude oil, lubricants and liquefied petroleum gas. Markers can also be used to identify and differentiate road fuel and subsidized fuel. The road and subsidized fuel products may be exactly the same from a chemical composition perspective. A fuel marker can be used as a "tax stamp" or "fingerprint" to authenticate the low tax fuel and validate (qualitatively or quantitatively) if it has been used as an adulterant in regular taxed fuel.

The fuel markers can be overt or covert. Overt markers such as coloured dyes can be visually authenticated in the fuel. Overt dyes can be used to mark subsidized fuel and its presence can signal the presence of an adulterant in the road fuels. Coloured dyes are typically more economical but are more susceptible to imitation, replication or laundering. Covert markers, on the other hand, are dosed into the fuel at low rates and are invisible. Proprietary devices and methods are used to detect the markers and determine whether any adulteration has occurred. Several different types of covert markers can be used, including:

- **Recognition markers:** they are captured by custom-matched antibodies and are then detected by a reader or test kit. Detection can be in the field (qualitative) or in the laboratory (quantitative). Industry-accepted and commercially proven, these markers provide a substantial barrier to entry and use low marking levels.
- **Optical markers:** they use covert organic chemicals that emit a detectable fluorescent light when excited and are visible only with a highly sensitive field detection device that provides near-instantaneous results.
- **Molecular markers:** they exploit the unique mass spectrum of chemical entities, enabling lab-based qualitative and quantitative analysis using forensic lab devices such as Gas Chromatography-Mass Spectrometer (GC-MS).

This submission also presents several options for fuel analysers, which include:

- **Portable Field Analyser:** A portable field analyser designed to detect non-launderable and environmentally safe markers. This is a self-contained portable device that is also easy to use for field inspections. Results are instantly stored in a secure, cloud-based database.
- **Field Test Kit:** Called Lateral Flow Device (LFD), it is a simple field test designed to give terminal operators and station owners quick results in the field to indicate whether the fuel is meeting specifications.
- **Fuel Quality Analyzer:** The fuel quality monitoring solution is designed to increase the speed of commerce and decision-making by reducing the time and cost of fuel quality testing and inspection. The solution uses field-based equipment and sophisticated chemometric modelling to provide near instant quality testing and a more robust, rapid, efficient and affordable alternative to traditional testing programmes.
- **Forensic Lab-Based Analyzer:** This system isolates the different components of fuel, and quantitatively measures the forensic marker. This forensic Gas Chromatography-Mass Spectrometry lab-based fuel marker analyser allows governments and oil companies to confidently take action against those committing fuel manipulation and fraud.

The solution can be used to streamline fuel quality testing and inspection, reducing both time and costs. This option uses mobile, field-based equipment and sophisticated chemometric models and machine-learning techniques to provide near-instant quality testing results and a more rapid and efficient alternative to traditional testing programmes. As more samples are processed, the system uses machine-learning capabilities to compare laboratory conformity results with field sample results, thereby improving the accuracy of field results and progressively bringing them closer to laboratory-quality standards. In this regard, the fuel quality monitoring solution can provide relevant information, such as:

- **Compositional Matching:** The material's relational composition and its change at different measurement locations in the same supply chain, which also confirms whether the material's profile matches a known or predicted profile based on the product type and supply source.
- **Material Identification:** It indicates whether the sample includes unleaded low-octane or high-octane gasoline, as well as diesel.
- **Adulteration:** It can be used to determine whether the fuel is adulterated, identifying the adulterant that was added, the level of contamination or the percentage of the adulterant with respect to the total sample.
- **Property Prediction:** Through analysis such as octane rating and sulphur content, it can determine whether the fuel at a retail location matches that from the appropriate terminal source.

The solution also has the capacity to integrate variable sample data results into a cloud-based information system, giving the user a single window for complete visibility into supply chain quality integrity and programme performance. Moreover, the technical solutions utilize GPS navigation and/or coordinates for logging sampling and testing of petroleum products throughout the supply chain. The adoption of traceability systems (such as IoT sensors) that can be deployed throughout the supply and distribution chain to track and trace petroleum products and monitor and report in (near) real-time enables the tracking of in-transit products (equipping trucks with GPS locks and security seals at loading points). Additionally, volume/ inventory sensors for monitoring fuels in the bulk storage tanks report volume fluctuation activity in an integrated solution, which also includes point-of-sale data as well as data obtained from loading facilities.

An additional feature that can be added is blockchain technology, which can serve as an effective solution for detecting the falsification of paper-based transport documents for fuel. A blockchain could be used to carry the complete audit trail in the various production processes. For example, the specifications, batch, and quality control results for fuels and additives can be recorded as they are produced according to accredited suppliers' quality management systems. While a ledger provides a record of a series of steps or transactions involving digital data, the generation of data such as test results, certifications, or volumes of a product

shipped between parties is also carried out in a manner that ensures the authenticity of the data produced. As in other supply chain solutions, the key is to design the protocol by which the physical-to-digital transformation of data is robust to avoid accepting falsified data.

Applicability to Limit Risks Included in the Scenarios

Scenario	Applicability of the solution
Scenario 1: *Infiltration into the supply chain*	
Step 1 – Political and economic infiltration.	
Step 2 – Infiltration into the legitimate supply chain.	Where a marking method can be applied to crude oil.
Step 3 – Infiltrating / controlling refineries.	The technology solution offers diverse tools for analysis to corroborate the authenticity of fuel. The field-based equipment and chemometric machine learning capabilities can be used to obtain instant quality testing results, enabling the identification of lower quality fuel. Testing could be performed in almost any context. If the fuel marking programmes (markers, analyzers, information systems) are applied, authentic fuel can be protected from the infiltration of counterfeit products. If additional technology solutions, such as blockchain-protected platforms and traceability systems are also implemented, the risks can be significantly mitigated.
Step 4 – Organizing a "cheap fuel trade".	As described above, the use of covert markers is a tool to detect dilution, substitution or quality issues. The low-quality fuel that is infiltrated can be detected during field inspections. Original fuel can also be protected through the adoption of IoT sensors in the track and trace system to monitor the different stages of the product in the supply chain. Blockchain technology would protect data exchange.
Step 5 – Infiltration into public procurement.	

Scenario	Applicability of the solution
Scenario 2: *Fuel laundering and mixing*	
Step 1 – Smuggling.	If the receiving country has a fuel control programme in place, this step of the criminal plan can also be limited since routine checks may identify smuggled fuel.
Step 2 – Fuel laundering.	Markers can be designed to resist laundering techniques such as heat treatment, clay, charcoal, acid wash, among others. In addition, field testing can be used to identify the infiltration of lower-quality fuel or fuel that is not compliant with applicable regulations and laws.
Step 3 – Mixing and distribution of adulterated fuel.	As previously described, the combination of markers for authentication and the use of field inspections for testing provide a tool to protect original fuel and detect counterfeit products. Data trends can also be analyzed to provide comprehensive insights into possible issues.

Technology Submission 2, by SICPA

The submission proposes the implementation of a Fuel Integrity Programme (FIP) intended as a turnkey solution to fight all aspects of fuel fraud. The FIP is a package of integrated services assuring the quality and traceability of the fuel products as they move through the supply chain using a marking technology. The FIP is composed of three main activities:

1. Marking of fuel.
2. The inspection to determine the level of the marker in the products in the field and the collection of all data pertaining to these two processes.
3. The subsequent reporting.

The strategy proposed consists of adding a covert molecular marker to taxed fuel so that it can be monitored and traced. Various technologies can be used for fuel marking; therefore, the most appropriate and optimized marker and detection equipment can be chosen to help the specific country achieve its policy and strategic objectives. The markers are invisible molecular markers, injected at very low concentration rates (few ppm) and cannot be copied, laundered, removed or altered. They are compatible with all types of fuel, stable at extreme temperatures with a long shelf-life and have no impact on car engines or emissions.

The solution proposes services that are fully coordinated and controlled to ensure their execution. Experts will deal with the marker logistics, security, stock management and transportation. Resources will be deployed for marking fuels, collecting samples for inspection and testing management, the issuance of test reports and data analysis to provide intelligence and risk information about illegal activity.

The inspection process provides a quantitative determination of marker concentration in fuels starting from 5% adulteration. Mobile field inspection units are usually installed in utility vehicles, allowing controls to be performed anytime and anywhere. Fuel test results are available in a few minutes and transmitted in real-time to the central database. Fuel test results are court-admissible. No additive, chemical reagent or physical manipulation is necessary, guaranteeing the integrity of the sample. Fuel test results are protected, automatically transmitted and videotaped, guaranteeing full traceability of the sampling and test integrity. They can be performed through a portable field fuel analyser, which can also precisely measure quality indicators (e.g. the presence of lead, sulphur or manganese in the sample.

Thanks to the network of experts established by this approach, checks can be conducted at designated sites to verify whether taxed fuels have been diluted. In addition, the fuels can be tested at mines or other industrial sites where the possibility of fuel fraud exists, and test results can be produced in a few minutes. The test detects, with a high level of accuracy, the levels of dilution or adulteration, or simply the presence of the marker; this provides authorities with evidence to support enforcement actions or legal prosecution.

Track and trace technology is also used along the supply chain, allowing data analytics to perform mass-balance calculations to detect fraud or diversion.

This submission also stresses the need to use technology to create trust in the overall hydrocarbon ecosystem. This can be achieved by providing a system that can deliver trust in data for rapid and independent verification in real-time, secure communication between actors and stakeholders (human, systems or connected devices), trust in the business processes and in the identity of the actors (immutable records and process integrity) and functionalities developed for supply chains such as track and trace, event provenance and automated business processes.

Measures can also be also put in place to protect the mass-balance equation[2] for any oil and fuel supply chain. The mass-balance equation refers to the volumetric-balance of product moving between departure and arrival points. There is a measurable set of volumes (Ve) of substances (crude oil, refined oil, lubricants) that enter a complex supply chain or a subset of it. Most of the time, governments must reconcile these volumes to calculate excise duties and other tax revenues. They rely on data (De, Dx) recorded along the supply chain. Problems occur when the final volumes exiting (Vx) differ from the initial ones (Ve) after adjustment for expected losses (L1). Smuggling, counterfeiting, diversion and other manipulations affect the fuel volumes and can result in unexpected losses (L2).

$$Ve = Vx + Lx$$

$$Lx = L1 + L2$$

2 Defined in the submission as the volumetric balance between departure and arrival points. Please, refer to the full description included in the report for more precise information.

Reconciliation would become easier and more efficient if the volumes measured (V) could be protected by chemical fingerprints or in-product tracers and if, in parallel, data (D) from departure to arrival points could be authenticated, recorded and secured in a blockchain.

In addition, space technologies can be used for proof of origin as well as for track and trace.

There are three main applications for the fuel supply chain:

1. **Proof of origin and mass balance:** Images from drones and satellites can be used to link products to their place of origin. They make it possible to calculate production volumes, to anticipate and facilitate reconciliation, that is, to verify whether the quantity of products in circulation is greater or smaller than the effective and verified original quantity.
2. **Quality:** Product quality can be assessed using specific imaging technologies including hyperspectral cameras.
3. **Monitoring and communication:** Spatial monitoring of land areas or vessels at sea has been used for a while, in some cases to detect criminal operations. Together with proof of origin, it provides additional data to check mass balance along the supply chain. Secure communication and data exchanges between drones, satellites and ground IoTs devices are key for supply chain auditability.

As space data is used for continuous and additional controls along the supply chain, data and processes must be certified and timestamped in a blockchain to avoid falsification. Compressed spatial images with their embedded unforgeable signatures and localisations through quantum derived technologies represent the next generation of solutions to be used in this regard.

Applicability to Limit Risks Included in the Scenarios

Scenario	Applicability of the solution
Scenario 1: *Infiltration into the supply chain*	
Step 1 – Political and economic infiltration.	
Step 2 – Infiltration into the legitimate supply chain.	In the case where markers could be applied to crude oil, the technology could also limit this step of the criminal plan.
Step 3 – Infiltrating / controlling refineries.	The solution can be used to detect when the criminal organization mixes cheap fuel with regular fuel, since the composition of the legitimate fuel is linked to a chemical fingerprint creating the identity of the product in the traceability system.

Scenario	Applicability of the solution
Step 4 – Organizing a "cheap fuel trade".	The technology solution can be used to detect mixtures composed mainly of gasoil and other added compounds that modify the final physical features of the product. The marking process in the Fuel Integrity Programme (FIP) protects the composition of fuel and secures it in the traceability system. The use of the solution adds layers of security if compared with more traditional approaches, including data analysis of product flow mass balances, supported by blockchain technology and the use of space technology to add additional time-stamped controls on the origin and quality of products and of their components, as well as to support the mass-balance calculations. Furthermore, the use of rapid portable on-field testing devices would make it possible to identify illicit fuel in cases of infiltration.
Step 5 – Infiltration into public procurement.	
Scenario 2: *Fuel laundering and mixing*	
Step 1 – Smuggling.	The various elements of this technology would allow the identification of illicit fuel in the country of destination, provided that the latter has a Fuel Integrity Programme in place.
Step 2 – Fuel laundering.	As previously described, the technology solution can protect the supply chain from the infiltration of counterfeit products. The use of invisible molecular markers, injected at very low concentration rates (few ppm), provides a means of authentication, as these markers cannot be copied, laundered, removed or altered, and are compatible with all types of fuel. Marking can later be verified through field inspections.
Step 3 – Mixing and distribution of adulterated fuel.	The technology solution can be used to detect adulterants and other added compounds that modify the final physical features of the product. The marking process in the Fuel Integrity Programme (FIP) protects the composition of fuel and secures it in the traceability system. In addition, security is increased through data analysis of product mass balances, supported by blockchain technology and the use of space technology to add additional time-stamped controls on the origin and quality of products and of their components, as well as to support the mass-balance calculations.

Technology Submission 3, by Nano4u

The submission provides a technology solution to mitigate risks related to the falsification of paper-based transport documents for mineral oils by using blockchain and secure immutable registries, including barcodes applied to shipment containers where relevant. The paperwork used during the supply chain usually includes barcodes which are scanned each time there is a change of ownership or location of the product, or when it is aggregated or de-aggregated from a batch of containers. Changes in ownership of the product and aggregation and de-aggregation of containers in larger shipments are recorded immutably in the blockchain. Cryptographic keys are exchanged, allowing the receiver to become the new owner of each item when authorised to do so by the sender. Each transaction is recorded as a new block.

A falsified or duplicated code that is introduced on false paperwork will not function in the blockchain because every code is linked to the previous supplier (holding an authorised cryptographic key) and to the next authorised owner after the exchange of cryptographic keys.

For tracing or checking historical information, a bridge-database can be used where the original unencrypted data resides. The bridge-database sits between the original scans and the blockchain, and its contents are hashed in groups into the blockchain so that they become immutable. A trusted computing platform is used for secure interfacing with Enterprise Resource Planning (ERP) systems and other internal systems of manufacturers.

The location and time stamping can be used in different ways, e.g. to cryptographically sign codes so that they cannot be faked, or simply to make a code unique by encrypting the time and location together with other relevant data.

An additional blockchain function uses a balance ratio between inputs and output that is recorded on the blockchain. This would require legitimate suppliers to log their shipments to the blockchain. If the amount of fuel and containers coming in was monitored (geographical satellite data would strengthen this), it should match a particular amount of packaged fuel output. If the same output is occurring but with a lower volume of authorised inputs, this suggests an issue. The bridge-database and blockchain solution with a trusted computing platform allows for a full and safe integration of ERP and other existing enterprise tracking and tracing software.

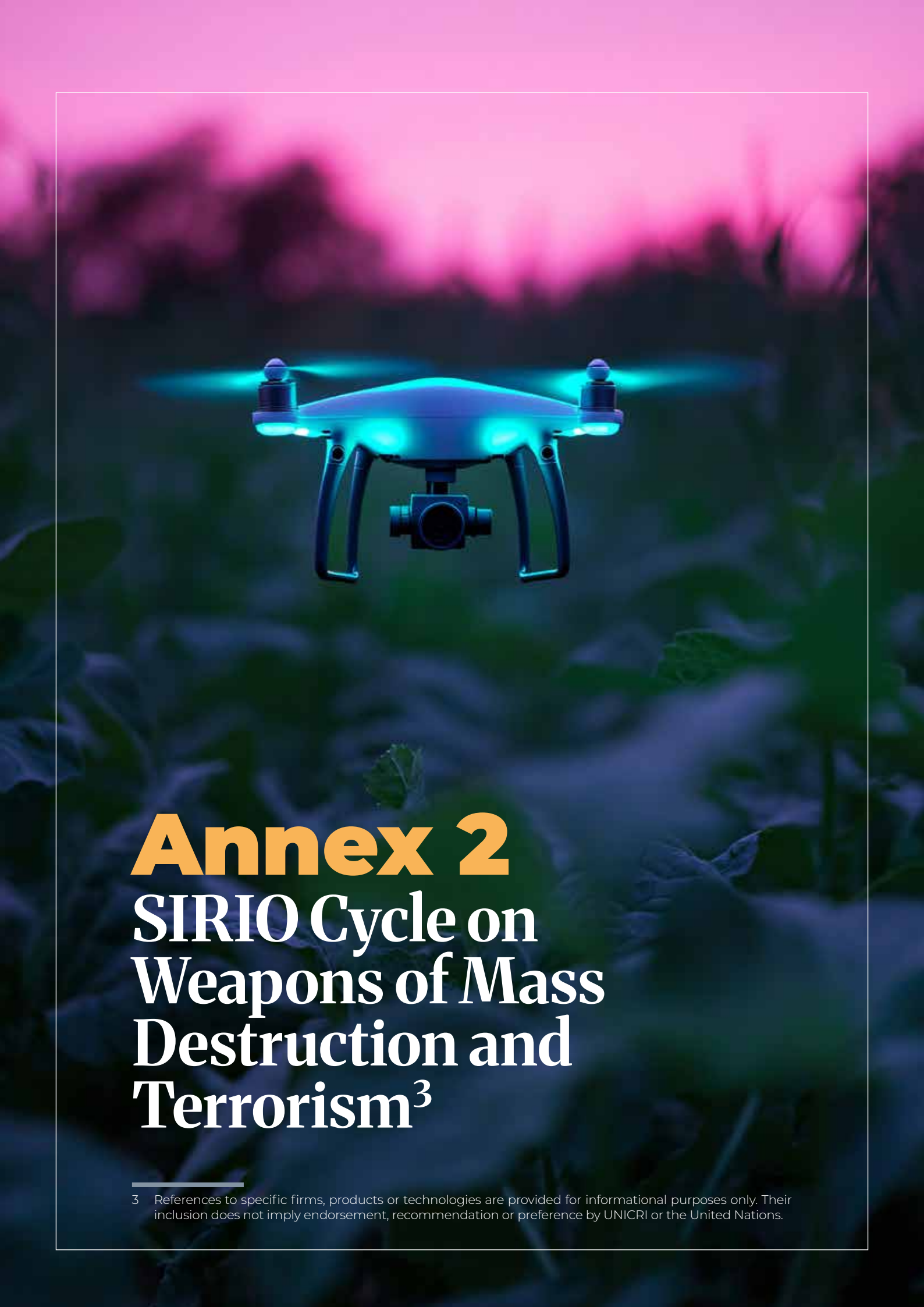
To transfer ownership of the product to the next supply chain point or to the end user, the sender must have both the authorised relationship with the next owner (via the exchange of cryptographic keys) and a valid barcode to scan, which is traceable through the bridge-database linked to the immutable blockchain. As a result, fake containers with fake or copied barcodes cannot be used.

Data from the bridge-database can be hashed together in different ways, providing higher information security for companies (e.g. there is no way for third parties to determine how many original data transactions they are making). If an attempt is made to change any entries in the bridge-database, resulting in a change in the blockchain, warning notifications can be configured to notify only those who need to know for security purposes, without alerting those earlier in the supply chain that their actions have been discovered.

The precise location and time data from satellite navigation and communications can be used (a) by embedding this information into data stored in a database and blockchain for current and historical tracking and authentication purposes, and (b) to provide a unique cryptographic stamp for printed codes that makes each code unique. With advanced systems, position data is many times more accurate than before, allowing such data to be highly reliable and effective even in environments with tall buildings. Without this space-related data, it would not be possible to track the origin and the location of products as they are packaged or repackaged.

Applicability to Limit Risks Included in the Scenarios

This submission focuses on ensuring that documents related to fuel transactions, including barcodes affixed on containers, are original and properly secured and transmitted. It does not have a way to authenticate the fuel itself and it may have a more limited immediate risk reduction effect for some of the most relevant steps of the criminal plan identified by the two risk scenarios. For this reason, a summary table at the end of the description was not inserted. However, the submission is interesting because it can work as an additional element improving the security of the supply chain by verifying that fuel transactions are authorized at any point of the supply chain by verifying related documents and containers. It is a similar approach used in the case of many other product categories where the focus of the protection is on the packaging and not on the product which is contained by the package.



Annex 2
SIRIO Cycle on Weapons of Mass Destruction and Terrorism[3]

3 References to specific firms, products or technologies are provided for informational purposes only. Their inclusion does not imply endorsement, recommendation or preference by UNICRI or the United Nations.

Examples of Risk Scenarios

Risk Scenario 1: Chemical Attack with Drones

In the near future, in the Republic of Blueland, a terrorist group believes that the government is corrupt and is betraying the core values of the country. They are convinced that an indiscriminate attack against the population would demonstrate the weakness of the Prime Minister and expose the government to public embarrassment and ultimately lead to its collapse.

To achieve this objective, the terrorist group decides to perpetrate an indiscriminate attack against the population during a political rally for the Prime Minister by using several drones to release a toxic chemical agent over Central Square – a large public square, located in Blueland's capital and surrounded by popular shops and restaurants. The terrorist group takes the following steps:

1. **Acquisition of chemical material:** The terrorist group purchases fumigants (gaseous pesticides used to control pests in agricultural fields) from a company that has been infiltrated by organized crime.
2. **Acquisition of drones:** The terrorist group purchases two types of drones: six large drones fitted with 20-litre tanks for carrying fertilizers or pesticides and six small drones (including drone-related components such as remote controls, lithium-polymer batteries, antennas, heat-activated film, etc.) from different companies located in different countries, arranging for the components to be delivered to several different addresses.
3. **Weaponization of the drones:** The terrorist group modifies and weaponizes the drones: the six large drones are weaponized with the aerosol canisters containing the chemical agent, while the six small drones are weaponized with improvised grenades.
4. **Identification of the target:** The terrorist group identifies a list of political rallies that will be held by the Prime Minister in the next few months during the upcoming re-election campaign. Large crowds are expected to attend each of these events. To maximize the impact of the attack, the identification of the specific rally to be targeted will be based on crowd numbers and weather conditions on the day of the event.
5. **Preparation:** On the day of one of the largest rallies of the re-election campaign – a rally at Central Square, where the Prime Minister is scheduled to address 5,000 supporters – the environmental conditions are favourable (no heavy rain and no strong wind) and the terrorist group launches the attack. Twelve individual pilots launch the twelve drones from a parking lot located close to Central Square along a pre-programmed flight path.

6. **Attack:** The six drones (outfitted with improvised grenades) start the attack by dropping explosives in the lower part of the square, causing people to move towards the upper part of the square. The other six drones (outfitted with aerosol canisters) release the chemical agent in the upper part of the square where many attendees have gathered.
7. **Consequences:** The attack triggers panic and a sudden rush of the crowd towards the exit points, causing a stampede. Law enforcement reacts quickly and takes down the drones, but several people at the rally are killed or injured by the explosions and the crowd crush. Hundreds more are hospitalized due to exposure to the chemical agent (with symptoms such as blurred vision, coughing and a burning sensation in the nose, throat, and eyes). International media are present in the area and immediately broadcast the news globally. The attack has also caused significant financial losses. The terrorist group claims responsibility for the attack.

Risk Scenario 3: AI-Powered Cyberattack Against a Nuclear Facility

In the near future, the Republic of Blueland has developed nuclear power generation capacity. Two modern commercial pressurized-water-reactor nuclear power plants are the primary sources of the country's electricity supply.

The group "ANTINUC" opposes any form of uranium mining, nuclear power, and nuclear weapons in Blueland. The group has undertaken public protests and acts of civil disobedience. Frustrated by their failed attempts, they decide to scale up their efforts and to launch an AI-powered cyberattack against one of the nuclear facilities in Blueland.

ANTINUC wants to demonstrate that nuclear plants are dangerous and potentially out of control. Their objective is to manipulate the systems that control a commercial pressurized-water-reactor nuclear power plant, damage the nuclear reactor's core, and cause an off-site release of radiation.

Three data experts who are supporting the cause of the terrorist group, devise a plan of attack that employs AI-empowered malware. The terrorist group takes the following steps:

1. **Preparation (spear phishing attack):** The terrorist group, with the support of the hackers, uses a neural network that analyses popular social media data (i.e. Facebook, Twitter, Instagram) and studies the profiles of nuclear engineers. Subsequently, they target staff in the administrative and information technology network of the nuclear plant with two types of attacks:
   - They deliver targeted phishing emails that appear to come from a trusted source;
   - They write phishing posts on popular social media platforms that target users with the profile of nuclear plant engineers.

When the staff of the nuclear plant open the email or the posts, malware BlackEnergy 3 is silently installed on their computers.

2. **Preparation (data analysis):** The malware, using AI protocols to hide its signature, embeds itself in the network and escalates its access. In this way, the hackers can study the defence systems, identify vulnerabilities, and determine how to circumvent security systems and avoid triggering any alarm when the system is attacked.
3. **Attack:** The malware operates in three phases:
   - The malware causes a hardware failure (the failure of a feed-water pump). As a result, heat and pressure increase in the reactor coolant system. The reactor shuts down automatically and, within seconds, the power-operated pressure relief valve on the reactor cooling system opens, leading to a loss of coolant.
   - The malware stops the closure of the pressure relief valve so that the loss of coolant continues (the relief valve should normally close when the excess pressure is released).
   - The malware gives operators at the nuclear plant misleading signals concerning the level of water covering the core (the interface panel indicates that the valve is closed, when in fact it is still open). As a result, the operators reduce coolant flow rather than increasing it.
4. **Consequence:** The fuel overheats and the encapsulation fails, releasing volatile fission products into the reactor building and subsequently some inert radioactive gases are vented to the outside environment.

Risk Scenario 5: Deliberate Food Contamination Using CRISPR

In the near future, in the Republic of Blueland, an ideologically motivated terrorist group seeks to destabilize the national government by perpetrating a large-scale, sensational act of bioterrorism. Committed to "high-tech" terrorism, they seek to cause large numbers of casualties (morbidity and mortality), generate widespread fear, and increase the notoriety of the group, its capabilities, and its ideological beliefs. To achieve these goals, the group draws on the expertise of a radicalized senior scientist who has recently infiltrated a legitimate biotechnology company conducting advanced biological engineering projects. The radicalized scientist is eager to demonstrate his commitment to the terrorist cause by using his privileged knowledge and access to produce a sophisticated biological weapon drawing on state-of-the-art synthetic biology techniques.

The terrorist group takes the following steps:

1. **Acquisition:** The radicalized scientist, who regularly works with E. coli K-12 bacteria for legitimate biological engineering and industrial microbiology applications, downloads the genetic sequence corresponding to a gene encoding a biological toxin (causing acute toxicity) from an online database.
2. **Development:** Working after hours, the radicalized scientist synthesizes the toxin-encoding gene using an in-house DNA synthesizer, uses a Clustered Regularly Interspaced Short Palindromic Repeats (CRISPR) kit to insert the toxin-encoding gene into E. coli K12, and employs common laboratory culture techniques to produce large quantities of the bacteria.
3. **Weaponization:** The radicalized scientist prepares multiple liquid slurries containing the bacteria and delivers them to his co-conspirators to contaminate food and drink at one or more national sporting events in the following days.
4. **Preparation:** The terrorist group identifies an upcoming national sporting event at Blueland National Stadium (a stadium with a 75,000-person capacity), where vulnerabilities have been identified in the food supply chain used to provide basic ingredients to stadium food vendors.
5. **Attack:** On the morning of attack, two members of the terrorist group infiltrate the warehouse supplying ingredients to Blueland National Stadium's food vendors and contaminate basic ingredients, including vegetables, cheese, milk and pre-cooked meats. On the night of the sporting event, thousands of fans attending the sold-out event consume contaminated products.

6. **Consequences:** The next day, hundreds of individuals report to local hospitals with what appears to be severe food poisoning (nausea, vomiting and diarrhoea), including some individuals showing more severe signs (respiratory distress, muscle weakness and seizures) of acute toxicity. That evening, as a growing number of individuals report to local hospitals, the terrorist group uses social media to claim responsibility for the attack, warning that the group released a "genetically engineered" pathogen at Blueland National Stadium the previous evening, and that further attacks are imminent. The news results in an influx of individuals who fear they may have been exposed (the "worried well") at the national stadium, exceeding the capacity of local hospitals to respond. Blueland's national government launches a criminal-epidemiological investigation, and all mass gatherings (sporting events, concerts, etc.), as well as public transportation, are suspended until further notice.

Examples of Innovative Ideas and Their Applicability to the Risk Scenarios

This section of the Annex summarizes technology submissions received by UNICRI. A more detailed description of each technology is presented in the report, including additional information, graphics, figures and explanatory tables.

Innovative Idea 1, by OSDIFE

The objective of this idea is to harness the potential of big data analytics to produce knowledge that could support intelligence operations related to WMD counter-proliferation. In particular, big data analytics could be applied to reinforce open-source intelligence (OSINT), that is the method of gathering, analyzing and interpreting publicly available data.

The use of big data analytics with OSINT could improve the capabilities of Member States' security and law enforcement officials to prevent, monitor and trace the acquisition of dual-use items by terrorists, including unmanned aircraft systems (UAS) and their components, commercial synthetic DNA, dual-use laboratory equipment and downloaded rinderpest virus genetic sequence information (in line with the risk scenarios on the misuse of unmanned aerial vehicles and the misuse of synthetic biology technologies). The proposal also intends to address the problem of how to monitor and restrict the use of additive manufacturing to produce components that could be used to produce WMD and their means of delivery (in line with the risk scenario on the misuse of additive manufacturing). Observatory on Security and CBRNe Defence (OSDIFE) has already developed an Intelligence Platform for CBRNE Events and Asymmetric Threats through which it produces frequent reports on CBRNE events worldwide.

OSINT methodology is widely used by State security, law enforcement agencies and the military in the area of countering WMD terrorism. By employing free and non-classified sources such as traditional and online media (including social media platforms, blogs and online publications), public government data (i.e. assets confiscated from organized crime or terrorist groups), private sector data or commercial data (including financial and industrial assessments) and publications, it is possible to monitor risk factors related to WMD terrorism and proliferation such as:

- Activities, ideology and motivation of potential non-state actors;
- Relationships between criminal and terrorist groups and between them and States that provide any form of support to non-state actors that attempt to develop, acquire, manufacture, possess, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery;
- CBRN events of malevolent, natural and human-made accidental nature;
- The risk of illicit transfer, sale or trafficking of materials, systems and technologies, especially in regions and areas affected by political crisis, conflict and instability;
- The risk of hiring scientists and technicians or of infiltrating scientific laboratories by terrorist groups;
- The risk that organized crime or terrorist groups infiltrate relevant industrial activities, including the acquisitions of industrial, business and corporate structures, as well as patents of strategic or significant interest and importance in the field;
- Availability of CBRN knowledge, expertise and technologies that could be used for terrorist purposes, especially by avoiding or circumventing commercial restriction measures;
- Suspicious movement and transportation of specific materials, delivery systems, precursors and CBRN equipment.

Big data analytics could be used to better structure data and establish correlations between them, using semantic and structural data abstraction techniques (visual analytics concepts and advanced graph processing techniques) to create knowledge out of large datasets. By combining big data analytics with OSINT, State security and law enforcement agencies could improve their capacities to monitor and detect WMD proliferation, including the ability to:

- Uncover potential WMD terrorism and proliferation scenarios such as suspicious acquisition and procurement of technology, goods, software, services or expertise, or suspicious activities in the research, development and production of CBRN materials;

- Identify trends and better understand how illicit trafficking and proliferation networks conceal their activities, including through the acquisition and use of dual-use items, the concealment of the end-users of traded items, and the involvement of intermediary entities and associated financial transactions;
- Identify unknown correlations between terrorists and individuals operating within illicit trafficking and proliferation networks;
- Predict where illicit trafficking and proliferation networks will invest in the future and in which market sectors;
- Predict possible WMD terrorist attacks;
- Other relevant proliferation-related activities.

Applicability to Limit Risks Included in the Scenarios

Innovative Idea	1. The use of OSINT and big data analytics to prevent and detect WMD proliferation networks
Objective	Enhance the capabilities of State security and law enforcement officials to prevent, monitor and trace the acquisition of dual-use items by terrorist groups, including unmanned aircraft systems (UAS) and their components, commercial synthetic DNA, dual-use laboratory equipment and downloaded RPV genetic sequence information
Reference to risk scenarios	▸ Risk Scenario 1 – Chemical Attack with Drones ▸ Risk Scenario 2 – Chemical Facility Sabotage with Drones ▸ Risk Scenario 3 – AI-Powered Cyberattack Against a Nuclear Facility ▸ Risk Scenario 4 – Agroterrorism Exploiting Dna Synthesis Technology ▸ Risk Scenario 5 – Deliberate Food Contamination Exploiting CRISPR ▸ Risk Scenario 6 – Illicit Trafficking of Missile Components for Delivering Biological and Chemical Weapons
Advantages	▸ Improved decision-making (actionable insights) ▸ Efficient data analysis ▸ Speed
Limitations	▸ Algorithm bias ▸ Need for domain experts ▸ Analysis of unstructured data ▸ Digital divide ▸ Past data may not reflect future trends

Innovative Idea 2, by FBI

The WMD Directorate of the Federal Bureau of Investigation (FBI) is exploring the possibility of using distributed ledger technology to prevent, monitor and trace the acquisition of dual-use items by terrorist groups, including drones and their components, commercial synthetic DNA, dual-use laboratory equipment and downloaded rinderpest virus (RPV) genetic sequence information. The proposal also offers some actionable ideas on how to monitor and restrict the use of additive manufacturing to produce components that could be used in the manufacture of WMD and their means of delivery.

The FBI is working on the development of the Common Threat Information Exchange (CTIX), a digital platform that will enable industry to share suspicious inquiries regarding their products and facilitate the real-time sharing of this information with law enforcement agencies around the world.

This novel platform has the capacity to counter the proliferation of a broad range of WMD and associated delivery systems, such as UAS, by shedding light on suspicious procurement agents and their networks through worldwide industry reporting. This platform would enhance the knowledge of partner countries on suspicious activities occurring globally, allowing law enforcement agencies to interdict attempts by State and non-state actors to acquire WMD-related material and technology.

CTIX is an innovative and whole-of-community approach to reducing threats using an encrypted peer-to-peer network powered by distributed ledger technology. The immutability of the distributed ledger technology would allow industry and law enforcement to document suspicious inquiries from those seeking to purchase military-grade or WMD-related components. Moreover, this decentralized, peer-to-peer reporting structure could connect multiple industries together to form a worldwide network to share information on suspicious activities and build a stronger consensus against potential threat actors. Law enforcement agencies would benefit from this global network to detect patterns and trends, and to formulate the larger picture necessary to counter proliferation attempts anywhere in the world.

Applicability to Limit Risks Included in the Scenarios

Innovative Idea	2. Blockchain to prevent and detect WMD proliferation
Objective	Prevent, monitor and trace the acquisition of dual-use items by terrorist groups, including drones and their components, commercial synthetic DNA, dual-use laboratory equipment and downloaded RPV genetic sequence information
Reference to risk scenarios	▸ Risk Scenario 1 – Chemical Attack with Drones ▸ Risk Scenario 2 – Chemical Facility Sabotage with Drones ▸ Risk Scenario 3 – AI-Powered Cyberattack Against a Nuclear Facility ▸ Risk Scenario 4 – Agroterrorism Exploiting Dna Synthesis Technology ▸ Risk Scenario 5 – Deliberate Food Contamination Exploiting Crispr ▸ Risk Scenario 6 – Illicit Trafficking of Missile Components for Delivering Biological and Chemical Weapons
Advantages	▸ Secure share of information ▸ No Central Authority ▸ Identification of connections and patterns ▸ Identification of potential motives ▸ Automation & lower administrative burden ▸ Scalability ▸ Threat prediction
Limitations	▸ Misconceptions ▸ Challenges related to data sharing

Innovative idea 3, by the Center for the Study of Democracy

The objective of this proposal is to raise awareness on the potential misuse of synthetic biology by developing an interactive virtual 3D laboratory tour. The idea is designed for life science practitioners and academic institutions with a view to securing life science institutions and especially dangerous pathogens from both insider and outsider threats. UNICRI has already implemented a pilot project of interactive virtual 3D laboratory tours. The Center for the Study of Democracy is also working on Responsible Lab App, a game-like awareness-raising tool which seeks to promote biosafety, biosecurity, and dual-use bioethics competence in a user-friendly, interactive, and engaging manner.

3D technology can be adapted to recreate real environments in order to achieve various objectives. The proposed solution aims at enhancing awareness and knowledge about insider and outsider threats at life science institutions working with especially dangerous pathogens through the development of 360° virtual tours of laboratories with different biosafety levels (BSL), ranging from Do-It-Yourself (DIY) community laboratories (BSL1) to high-containment laboratories (BSL3/BSL4). To design the Virtual Reality (VR) solution, collaboration with laboratories will be essential to access facilities that will feature in the virtual laboratory tours.

The virtual tours would allow users to navigate through the laboratories and to click on selected equipment and areas to access more information (audio, text and video) on preventive and protective measures (physical protection equipment, authorisation and access to EDPs, laboratory design features, personnel reliability programmes, behavioural observation, etc.). Quizzes would allow users to self-assess the knowledge obtained, and scenarios involving security breaches by insiders and outsiders will be developed to provide users with practical knowledge on potential threats.

The virtual 3D laboratory would be based on a script and storyboard that would define the particular scenarios to be captured with a panoramic or 360-degree camera to create the required videos. The scripts can be translated in multiple languages; therefore, the recorded audio and narration should be designed to facilitate multilingual adaptation. Ideally, the tours would be accessible from both desktop computers and mobile devices.

In addition to raising awareness about biosecurity, the scope of the virtual 3D tour could also be expanded to the area of forensics, considering that the analysis and interpretation of forensic evidence requires close collaboration between law enforcement agencies and forensic scientists. In this connection, the application could also include virtual reality training materials on microbial forensics.

Applicability to Limit Risks Included in the Scenarios

Innovative Idea	5. Virtual Reality (VR) to reinforce biosecurity
Objective	Raise awareness of the potential misuse of synthetic biology by developing an interactive virtual 3D laboratory tour
Reference to risk scenarios	▸ Risk Scenario 4 – Agroterrorism Exploiting DNA Synthesis Technology ▸ Risk Scenario 5 – Deliberate Food Contamination Exploiting CRISPR
Advantages	▸ Interactive ▸ Immediate feedback and self-monitoring ▸ Flexibility ▸ Safety ▸ Enhanced awareness and preparedness ▸ Bridging the gap between theory and practice
Limitations	▸ Limited scope ▸ Costs ▸ Dependence on technology and infrastructure ▸ Data protection ▸ Limited interpersonal interaction

Innovative Idea 4, by SICPA

This idea proposes the use of a Fourier Transform Near-Infrared (FT-NIR) spectrometer to detect deliberate chemical contamination of food. SICPA Solutions has successfully tested a portable authentication device incorporating FN-NIR in this field within the framework of a European Union project.

The FT-NIR spectrometers are devices capable of obtaining simple, rapid and non-destructive measurements of chemical substances. These devices are based on the characteristic absorption or transmission spectrum of chemical bonds, which can be used to identify chemical compounds in the same way that a fingerprint can be used to identify an individual. FT-NIR requires no sample preparation and does not require the use of dangerous or hazardous chemicals, making it a fast, safe and dependable technology.

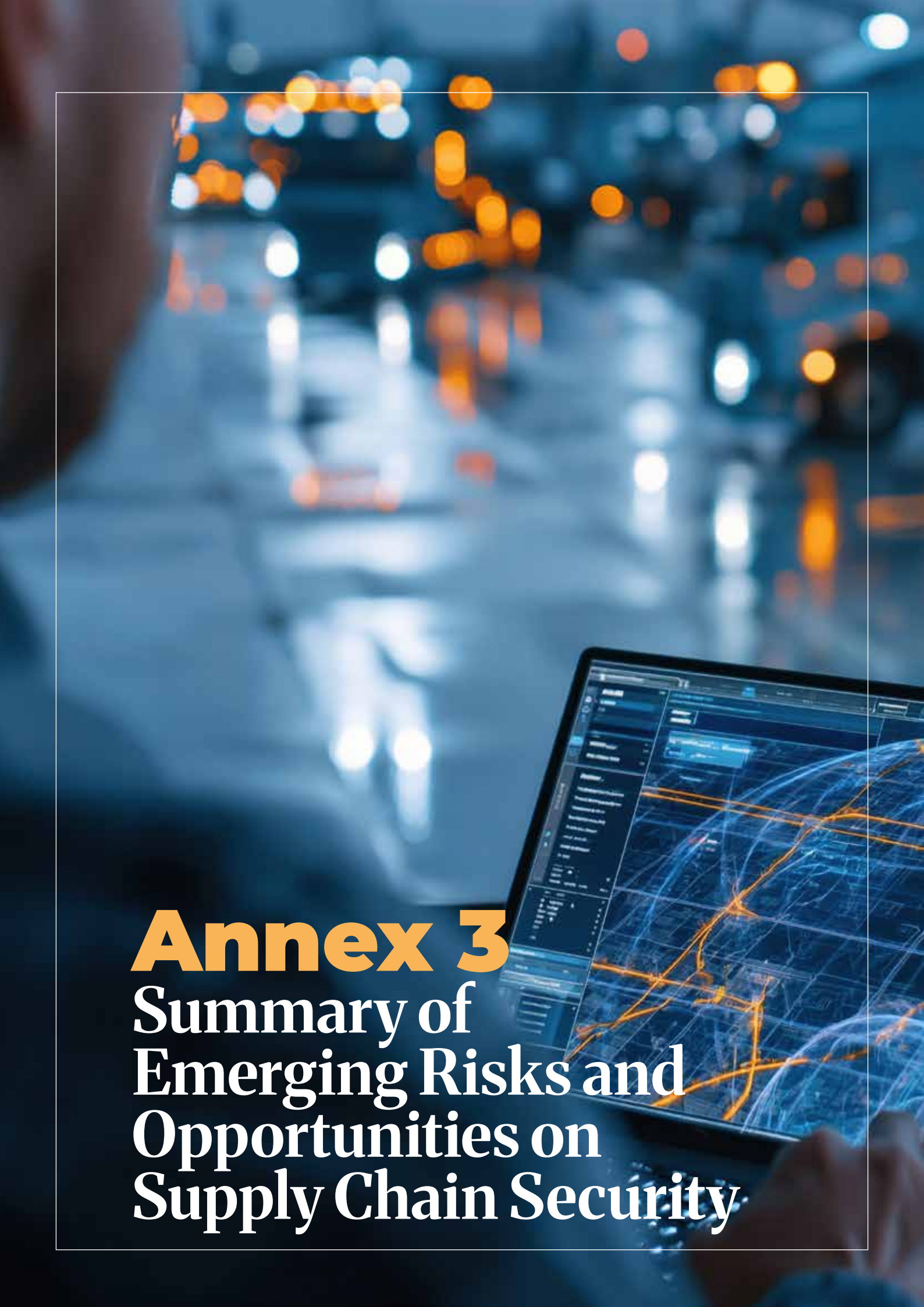
The FT-NIR spectrometer is effectively used in the food industry and agriculture to help ensure product quality and protect consumer health.

If applied in the area of WMD terrorism, the FT-NIR spectrometer can be used to detect deliberate food contamination with chemical materials. In particular, it can be used as a rapid first-screening device in cases of indiscriminate food contamination involving an unknown contaminant. By using a library of pre-defined test cases, the FT-NIR spectrometer can quickly detect the presence of a contaminant. In the event of a positive result, the samples should be analyzed with more targeted and time-consuming techniques (such as chromatography).

A portable authentication device equipped with a FT-NIR spectrometer can help law enforcement authorities make rapid decisions without the need to send samples to a laboratory for analysis.

Applicability to Limit Risks Included in the Scenarios

Innovative Idea	7. The use of an FT-NIR spectrometer to detect deliberate chemical contamination of food
Objective	Detect deliberate chemical contamination of food
Reference to risk scenarios	▸ Risk Scenario 5 – Deliberate Food Contamination Exploiting CRISPR
Advantages	▸ Easy to use ▸ Speed ▸ Low costs
Limitations	▸ Additional tests required ▸ Limited scope ▸ Limited sensitivity



Annex 3
Summary of Emerging Risks and Opportunities on Supply Chain Security

01 Criminal Infiltration Across the Supply Chain

Organized crime groups demonstrate the capacity to infiltrate legitimate supply chains at multiple stages through sophisticated and adaptable methods. These include the exploitation of technological vulnerabilities, corruption, theft, manipulation of packaging, and creation of parallel distribution channels. Such diversification allows criminal actors to compromise entire supply networks and evade detection. Addressing these risks requires a comprehensive, multilayered security framework that integrates a broad range of technological and procedural safeguards.

02 Criminal Control of Legitimate Operators

Certain criminal strategies such as the acquisition or covert control of legitimate businesses fall outside the scope of what supply chain technologies can prevent. When criminal groups gain ownership or effective control of operators, they can bypass technological safeguards and manipulate supply chains from within. Mitigating these forms of infiltration necessitates enhanced law-enforcement interventions, intelligence-driven monitoring and strengthened regulatory oversight. These elements are essential to identifying and disrupting criminal structures embedded in legitimate commercial activities.

03 Fragmentation of Technological Solutions and the Need for Integration

The complexity of supply chain vulnerabilities requires the integration of multiple technological tools rather than reliance on a single solution. Technology submissions received by UNICRI demonstrate a growing trend toward combining authentication features, traceability systems, massbalance verification mechanisms and other secure technology tools to reinforce product security. This multilayered approach enhances resilience and increases the likelihood of detecting counterfeit or diverted goods. Effective implementation, however, requires sustained cooperation among authorities, investigators, privatesector actors and consumers.

04 Limited Consumer Awareness of Authentication Mechanisms

Although authentication technologies are increasingly accessible often through simple smartphone-based verification consumer awareness and use of those technologies remain insufficient. The effectiveness of authentication systems would increase if the public's ability to recognize verification tools and understand how to use them correctly were more widespread. Low consumer engagement weakens last-mile protection and permits falsified goods to circulate even in regulated markets. Strengthening consumer education is therefore essential to enhancing the overall integrity of supply chains.

05 Expansion of Online Marketplaces as Vectors for Illicit Trade

The rapid growth of online markets, social media platforms and ecommerce channels has created new opportunities for organized crime to exploit them and distribute falsified and illicit products. Difficulties in monitoring, limited datasharing between online marketplaces and law enforcement agencies, as well

as gaps in cooperation with payment service providers may facilitate illegal activities. Strengthened digital surveillance, enhanced financial-tracking mechanisms and improved coordination between law enforcers and online platforms are critical to addressing these emerging risks.

06 Insufficient Integration of Forensic Analysis into Enforcement

Forensic techniques especially nuclear and chemical analytical methods play a crucial role in identifying the origin, composition and authenticity of goods after a breach occurs. However, forensic capabilities are often underutilized or inconsistently integrated into national and regional enforcement strategies. Limited access to laboratories, insufficient reference databases and the lack of portable tools constrain the ability of authorities to trace illicit flows and present scientifically robust evidence in court, weakening deterrence and prosecution outcomes.

07 Cross-Border Evasion and Transshipment Tactics

Criminal networks circumvent enforcement by mislabelling and repacking goods, forging distribution documents, and routing shipments through lowerrisk borders and complex maritime corridors. These practices obscure origin and custody, fragment risk signals across jurisdictions, and delay enforcement actions. Targeted customs risk-profiling is key to disrupt these evasive logistic practices.

08 Operational and Evidentiary Constraints of Field Testing

The expansion of portable, onsite screening tools improves coverage of screening activities conducted on suspect goods. However, when not properly implemented, these tools can also introduce risks of inconsistent calibration, false positives/negatives and chain-of-custody gaps. Without standardized protocols and confirmatory laboratory pathways, results may be challenged in court and under-utilized operationally. Clear evidence admissibility guidelines and proficiency testing would support translating on-field screening into enforceable evidence.

09 Insertion and Commingling at Intermediate Nodes

Illicit products are often introduced at consolidators, warehouses or distribution hubs where verification is weakest and volumes are highest. Commingling with legitimate stock complicates product attribution and recall. Risk-based intermediate checkpoints, secure custody controls and mass-balance reconciliation at transfer points can support closing this gap.

10 Environmental and Public-Safety Risks from Illegal Unloading and Storage

Unregulated depots, clandestine unloading points and unsafe storage practices heighten the likelihood of spills, contamination and fires. Such sites typically evade inspections and lack emergency preparedness, creating disproportionate local hazards. Remediation burdens fall on public authorities while polluters remain hidden. Strengthened site surveillance, rapid closure powers and liability mechanisms are needed to deter these operations.