UNDERSTANDING AND MAXIMIZING C-IED INFORMATION SHARING

By Paul Amoroso, an explosive hazards specialist at Assessed Mitigation Options (AMO) consultancy

INTRODUCTION

According to Dr. Sani Adamu, Programmes Officer, Disarmament and Arms Control, ECOWAS, who is involved in regional C-IED efforts[1] in West Africa, "before you counter a problem, you need to know the problem."[2] In the case of C-IED this refers to understanding the use or threatened use of IEDs, so that in time effective and efficient C-IED efforts may be invested in as part of a C-IED enterprise[3] to at least match but ideally overmatch the IED threat. This article is part of a series which examine strategic regional and national approaches to C-IED, based on research conducted by the author as part of an MA in Strategic Studies which explored and identified C-IED strategic principles for East Africa. This article will seek to outline what is meant by obtaining an understanding of the IED threat faced and how the development and sustainment of an accurate IED threat picture[4] can support this. It will examine why the near constant mantra of the importance of information exchange in support of C-IED is critical to such understanding. We will then look at two examples of what can be considered success stories in support of international efforts to better understand and then counter the threat posed by IED use with the World Customs Organization (WCO) and the International Criminal Police Organization (INTERPOL).

UNDERSTANDING

The criticality of understanding in support of any coherent C-IED enterprise is both cross-cutting and multi-dimensional. Understanding refers to the need to comprehend inter alia:

- Why and how IEDs are used;
- Use of appropriate terminology;
- What a national C-IED enterprise entails;
- Maintaining an accurate IED threat picture for effective C-IED decision making;
- Role and importance of exploitation in maintaining an accurate IED threat picture;
- Timely information sharing between C-IED stakeholders;
- Appropriate classification of C-IED information.

Understanding Why and How IEDs are Used

Understanding why IEDs are used refers to an appreciation of the root causes which lead to the insecurity and instability that facilitate their use. This is important when seeking to develop coherent C-IED enterprises as it is only after we establish the baseline factors contributing to their use, can we be appropriately informed to know what C-IED efforts we should invest in as part of coherent C-IED enterprises. Ultimately, understanding why IEDs are in use is key to successful efforts to counter them through a coherent, coordinated, and complementary[5] whole of system approach.[6]

How IED threat actors[7] achieve target effects is by the ways they are employed and the modus operandi of their organisation. Being versatile, IEDs lend themselves to a wide array of employment methods. An understanding of IED employment methods in use is necessary to inform what must be implemented to counter them and support optimised risk mitigation. IED employment methods can be considered on the strategic, operational, and tactical levels. At the strategic level, IEDs are a tactical asymmetric weapon system with strategic impact, being an excellent weapon of irregular or hybrid warfare which support the intention to destroy an opponent's political will to fight. At an operational level examining how IEDs are employed involves an examination of the IED system[8] which considers the network[9], processes and material involved in IED attacks and is then related to their modus operandi, strengths, weaknesses, opportunities, constraints and limitations. At the tactical level, we may pose the question 'how IEDs are emplaced and used tactically' which informs their tactical characterisation, referring to the way IED attacks are planned and conducted (tactical design[10]) along with their intent (purpose of the device). IED tactical characterisation of an IED attack provides context for how a specific device is used or intended to be used. The methods of employment of IEDs vary depending on the intended effect that an IED threat actor wants to achieve along with the constraints they face due to the C-IED efforts implemented.

There are no fixed templates for IED tactics due to their versatility coupled with their complex, dynamic and evolving nature. This combines to make the method of employment of IEDs extremely wide ranging and often unique to a given area. However, recurrent commonalities in IED tactics can develop as threat actors attempt to achieve the same tactical intent in a given area of operation. Such common IED tactics can be identified through appropriate analysis allowing effective C-IED measures to be developed. It is important that reliable and systematic methods to track such tactical patterns are developed and maintained as part of the system supporting the IED threat picture.[11] As effective IED countermeasures are implemented, IED threat actors adapt their methods of employment to circumvent the countermeasures introduced. This often becomes the action-reaction-counteraction cycle between IED threat actors and C-IED stakeholders, which is the reason why maintaining an updated IED threat picture is essential requiring on-going timely information sharing between all C-IED stakeholders.

Use of Appropriate Terminology

The issue of IED use being dismissed as too complex to allow effective C-IED efforts being implemented may partly be due to 'mystery by misunderstanding.' Such a lack of understanding can lead to an acceptance of defeat. This mystery surrounding IED use can be compounded by the use of inconsistent and often unnecessarily technically complex language for the target audiences being communicated with. Despite the somewhat technical nature of C-IED, this may be addressed using clear, precise, and uncomplicated language, so that all stakeholders understand the threat as well as the C-IED efforts that collectively make up the C-IED enterprise being invested in.

What a National C-IED Enterprise Entails

When developing a national C-IED enterprise to inform the understanding of the IED threat along with the C-IED priorities, a baseline assessment of the current C-IED capabilities in place is required. A good starting point is the use of the UNIDIR C-IED assessment tool, which provides an honest and objective needs analysis of gaps in a nation's C-IED capabilities.

Maintaining an Accurate IED Threat Picture for Effective C-IED Decision Making

The most informed decisions can be made within any C-IED enterprise when they are evidence based. This is reliant on an accurate understanding of the IED threat at any given time. The US Army C-IED strategy[12] has an IED information and analysis line of effort whose end state is to "gain the knowledge required to operate effectively in environments where IEDs are

present." Accurately understanding the IED threat on every level is a critical prerequisite for planning the most effective preventative measures, as well as seizing the initiative and sustaining momentum. Decisions taken at the strategic level need to be appropriately informed by accurate intelligence products which require the sharing of C-IED information and its subsequent fusion so that the most accurate IED threat picture is established. According to the US Army C-IED Strategy to establish and maintain an accurate IED threat picture it is necessary to collect, process, and analyse IED related observations, trends, patterns, friendly force lessons learned and evolving threat information, with collaboration between relevant intelligence partners as well as establishing, maintaining, and supporting forums and repositories for the collection and sharing of IED information. However, establishing an accurate IED threat picture is caveated on the need for the acquisition of the correct C-IED information. At an IGAD security chiefs meeting on C-IED in February 2022, it was stated that there was a belief that the IED threat in general is under reported, mainly due to lack of joint reporting channels, non-systematic battlefield and military collection and limited forensics exploitation capacity.[13]

Role and Importance of Exploitation in Maintaining an Accurate IED Threat Picture

The issue of appropriate C-IED information acquisition is centrally based around the key C-IED activity of IED exploitation.[14] IED exploitation is a key enabler in any C-IED enterprise, as it provides the information which, through appropriate analysis and fusion, can become C-IED intelligence. This can empower an accurate IED threat picture and support investment in appropriate C-IED efforts to at least match but ideally overmatch the threat. It can also support efforts to attack the IED network[15] allowing supply chains to be targeted and perpetrators to be apprehended. IED exploitation is beneficial at all levels of a C-IED enterprise. For example, it can empower quick wins at the tactical level, by informing protective measures needed, at the operational level it can support the prosecution of IED threat actors, while at the strategic level it can inform legislation aimed at reducing access to IED components.

Timely Information Sharing Between C-IED Stakeholders

Information sharing between all C-IED stakeholders is a key enabler to success in efforts to at least match but ideally overmatch the threat posed. However, as an IED threat typically evolves due to the action-reaction-counteraction cycle that plays out between IED threat actors and those engaged in a C-IED enterprise, the collective efforts that make up a C-IED enterprise need to continually evolve. For a C-IED enterprise to remain effective and threat aligned it must be based on an accurate IED threat picture which needs to be supported by timely information sharing between its stakeholders.

Appropriate Classification of C-IED Information

One of the justifications often presented for a lack of C-IED information sharing is the security sensitivity of the subject matter. However, this can be overstated, particularly when IED TECHINT is mixed with HUMINT. This can often lead to over classification and handling restrictions placed on it resulting in restricted sharing. A balance is needed between HUMINT, focused on IED network actors, and TECHINT, focused on IED components, for understanding to be optimal.

CHALLENGES TO C-IED INFORMATION SHARING

There is a perception that the challenge faced in countering IED use is a complex intangible problem; however, through appropriate information exchange in support of a common understanding amongst stakeholders this challenge may be simplified and in effect demystified. A simple analogy used to emphasise the importance of information sharing as part of any effective C-IED enterprise is that the IED threat picture is made up of many sources which can be considered the pieces of a jigsaw. All the various pieces of the threat picture jigsaw are held by many of the stakeholders who are part of or should be part of a C-IED enterprise. The more pieces of an IED threat

picture jigsaw shared, the more accurate the resulting picture, providing stakeholders with a better understanding of the threat. The less information shared the less accurate the threat picture which in turn affects the ability to invest in the most appropriate C-IED efforts needed as part of an effective C-IED enterprise. However, there is often a reluctance to share C-IED information preventing its optimized centralized analysis in support of an accurate IED threat picture. While interagency information sharing within an IED affected state can be challenging, it is an even greater challenge between states. Some of the challenges faced in creating an information sharing culture amongst C-IED stakeholders include:

- Suspicion and lack of trust between C-IED stakeholders can arise for many reasons. Professionals involved in C-IED information handling and intelligence development are often by nature very cautious in sharing, owing to perceived security issues and often seeking to protect their sources and collection methods. For example, those within the security and defence communities may not trust those within the development, civil society or academic communities all of whom may have C-IED information and need access to the IED threat picture or significant portions thereof. This lack of trust is often based on the perception that such non-security or defence entities will not employ appropriate information handling restrictions on C-IED information potentially compromising sources and methods. This may inform IED threat actors on countermeasures needed to circumvent C-IED measures either in place or being developed. Similarly those not within a State's security and defence architecture may not want to share C-IED information owing to efforts to protect their impartiality or fear of reprisals for cooperating with the State.
- Interagency rivalry between those in information collection and subsequent product development can lead to less-than-optimal understanding.
- Variations in the standards between different C-IED stakeholders providing C-IED information to the threat picture can pose challenges.
- A further problem arises due to what may be considered the 'blackhole of intelligence' referring to the perception amongst those who undertake the risky activities of acquiring IED data to feed into the intelligence community to never receive timely feedback in an updated IED threat picture. Some refer to the perception of a lack of trust and respect from the intelligence community to those involved in IED exploitation. This often leads to frustration, resentment and subsequently a lack of engagement with IED exploitation activities. These issues may be even more pronounced when an IED affected state has foreign assistance providing IED exploitation and subsequent IED intelligence generation.

POTENTIAL SUPPORT FOR AN INFORMATION SHARING CULTURE AMONGST C-IED STAKEHOLDERS

The stakeholders involved in a C-IED enterprise need to communicate effectively and efficiently their respective intent, requirements and constraints with their community of practice. This needs to be further qualified in terms of the information they can provide, and that which they require and if it is at the technical / tactical level, operational level and/or strategic level. Individual stakeholders will have different information which they can provide to best support the maintenance of an accurate IED threat picture as well as the C-IED information they require at one or more of these levels to best support their C-IED decision-making processes.

The information exchange system that supports an IED threat picture needs to be secure and trusted by all stakeholders and timely in the passage of information between users. The security protocols need to reflect stakeholder constraints firstly in terms of limitations on the information they provide and its subsequent handling and secondly any internal constraints from within the organisation on what information they require, are allowed to access or are capable of handling. Owing to a variation in the respective requirements and constraints among stakeholders there may need to be a memorandum of understanding

between each of them, or alternatively a memorandum of understanding between each stakeholder and a centralised national authority responsible for coordination of C-IED information sharing such as a fusion centre.

Security protocols will also need to address issues which include IT infrastructure required and the security classification of various parts of the system and their interconnectivity internally and externally. For example, where on the system will HUMINT and related information be stored and accessible will possibly be different compared to that for TECHINT. However, certain elements of TECHINT such as directed explosive warheads or radio control switch specifications and capabilities may need higher security protocols compared to other TECHINT held on a given data base. Ultimately, the IT infrastructure will need to be segregated and compartmentalised to reflect different user handling requirements. Cyber security measures will also need to be implemented for such databases. When such security protocols are established, C-IED stakeholders who require access to it can have a high degree of trust in the system itself.

A second element of trust in C-IED information exchange, relates to the trustworthiness of the information which is on the system in terms of reliability of its source and credibility of the information. The adage rubbish in rubbish out is pertinent in this case. A robust system of fact checking and verification of data placed on such a database needs to be established for all contributors and users to be aware of and to implement. A system that assesses the reliability of sources and the credibility of C-IED information provided[16] is ideal for all C-IED information provided for an IED threat picture.

The need for timely C-IED information exchange in support of maintaining an accurate IED threat picture to allow the most appropriate C-IED efforts to be invested in as part of a C-IED enterprise has been acknowledged as challenging. This is a resource intensive process requiring dedicated appropriately qualified personnel empowered to share, supported by the correct IT support for secure exchange, analysis and storage and the budgets to sustain and upgrade these systems, processes and personnel competencies over time.

Finally, the recurrent theme of the lack of trust being an impediment to effective information exchange in support of an accurate IED threat picture can be reduced through the establishment of a network of liaison officers or dedicated points of contact between the stakeholders involved in a C-IED enterprise. Such liaison officers or dedicated points of contact can be full time or part time and can be bilateral between two stakeholders or act as the sole point of C-IED information exchange between its parent organization and all other stakeholders. In the case that many stakeholders within a C-IED enterprise have dedicated liaison officers, they would ideally be in a dedicated information exchange location such as an IED threat picture fusion centre.

WORLD CUSTOMS ORGANIZATION SUPPORT FOR DATA EXCHANGE[17]

Intelligence is a vital element of enforcement for customs services that are to perform control missions while at the same time facilitating trade. To prevent control and search operations from impeding the free movement of persons, goods and means of transport, customs services need to implement intelligence-based selective and targeted controls. Information exchange on potential or real risks of offences is therefore vital if customs services are to implement their enforcement strategy. An interesting example of the international exchange of information is the World Customs Organization (WCO) which provides a standardized approach to data exchange related to goods, transport and other trade-related activities between Customs administrations as well as other stakeholders involved in the international supply chain to help reduce delays, errors and costs associated with cross-border trade.

To enable its members to combat transnational organized crime more effectively, the WCO developed a global system for gathering data and information for intelligence purposes – the Customs Enforcement Network (CEN). Developed in 2000, CEN comprises a

global non-nominal database of Customs seizures and offences by the WCO and an encrypted communication tool facilitating the exchange and use of information and intelligence. CEN aim is the collection of data to enable the analysis of illicit trade, the identification of trends and patterns, and the creation of intelligence products. It offers the possibility of sharing and disseminating information on customs offences in a timely, reliable and secure manner with direct access 24 hours a day. The CEN offers customs officers access to:

- Database of (non-nominal) customs seizures and offences, comprising data required for the analysis of illicit trafficking in the various areas of customs competence;
- CEN website containing alerts as well as information of use to customs services;
- Concealment picture database of exceptional concealment methods and the exchange of X-ray pictures;
- Communication network facilitating cooperation and communication between customs services and CEN users at the international level.

The CEN contains 13 different headings and products covering the main fields of customs enforcement activity, three of which can support the development and sustainment of an accurate IED threat picture, namely, precursors, hazardous materials as well as weapons and explosives.

INTERNATIONAL CRIMINAL POLICE ORGANIZATION (INTERPOL)[18]

Another international organisation which facilitates information exchange that can support maintaining an accurate IED threat picture and associated C-IED efforts is the International Criminal Police Organization (INTERPOL). INTERPOL facilitates the sharing and access to data on crimes and criminals and offers a range of technical and operational support, ensuring that police around the world have access to the tools and services necessary to do their jobs effectively. Along with targeted training and investigative support, relevant data and secure communications channels are provided to its member countries via a communications system called I-24/7. Using I-24/7, INTERPOL National Central Bureaus can search and cross-check data in a matter of seconds, with direct access to INTERPOL databases, with instant access to potentially important information, thereby facilitating investigations. Member countries use this secure network to contact each other, and the INTERPOL General Secretariat. It allows real-time access to 19 databases and services, from both central and remote locations.

Within INTERPOL, the Chemical and Explosive Terrorism (CMX) Prevention Unit seeks to increase the capacity of INTERPOL member countries to deal with terrorists and criminals acquiring, diverting, smuggling and using chemical warfare agents, toxic industrial chemicals and explosive precursor chemicals. CMX activities are underpinned by a comprehensive system of intelligence gathering and analysis – known as Project Watchmaker. Project Watchmaker is a global initiative offering specialized support to member countries by using INTERPOL's notice and diffusions system to alert law enforcement officials worldwide about people using or manufacturing IEDs. This project is intended to enable INTERPOL member countries to identify and track known or suspected individuals involved in the manufacture or use of explosives. This is achieved via working groups that facilitate the exchange of biometric data and TECHINT document records by identifying and uploading profiles of known and suspected persons involved in the acquisition, manufacture or use of IEDs to a dedicated database. This database allows INTERPOL to assist law enforcement agencies in detecting the transnational movement and operation of IED makers and facilitators. The project seeks to enhance capabilities in IED prevention, preparedness, response and recovery. Project Watchmaker has developed a regional-based model in line with the current IED threats, which is derived from actual incident data. The data collected by Watchmaker is formed into a catalogue of devices that can be regionalized. Through patterns and trends, it is possible to compare devices in various regions and establish whether we are looking at an individual or

group, and if either have been educated using social media. Obtaining information across regions allows for detailed, analytical reports that can highlight capability gaps, IED trends, component parts and areas of acquisition. INTERPOL's Watchmaker dataset contains profiles of over 3,500 people and 38,750 entities associated with chemical, biological and IED activities. It includes individuals responsible for major terrorist bombing incidents around the world. Coordinated efforts coming out of Watchmaker working group activities have developed into the operationalization of data to support the overt and covert detection of bomb-makers as they cross international borders. INTERPOL uses a series of colour-coded notices to communicate IED-related information to its members. This alerts member countries to take appropriate legal action. This is achieved through operations at major but vulnerable, air, sea and land borders that train local officers in the use of databases and border controls skills.

CONCLUSION

We have explored the importance of and wide-ranging elements which contribute to effective understanding in C-IED. This understanding refers to the IED threat along with the various elements required for an effective C-IED enterprise. Developing, maintaining, and sustaining an accurate IED threat picture to inform the most effective C-IED efforts which collectively make up a C-IED enterprise is critical. This requires creating an effective and trusted C-IED information sharing culture amongst C-IED stakeholders which needs to overcome several often typically encountered and persistent challenges. However, through effective C-IED stakeholder communications within the community of practice, establishing a trusted information exchange system, which supports timely C-IED information exchange, through a network of liaison officers or dedicated points of contact ideally working within an IED threat picture fusion center, an effective and trusted C-IED information sharing culture amongst C-IED stakeholders can be established. The WCO CEN and various databases of INTERPOL as well as its Project Watchmaker are examples of effective information sharing in support of C-IED understanding.

NOTES

1 C-IED efforts refer to all initiatives, activities, assistance, capabilities and capacities that collectively make up a C-IED enterprise. C-IED efforts can include inter alia, training, mentoring, advising, accompanying, assisting, technology and equipment (T&E) provision and intelligence support.

2 Interview conducted by author in 2022 as part of research on this topic.

3 C-IED enterprise is the collective term to describe all initiatives, activities, assistance, capabilities, and capacities that contribute to the C-IED efforts intended to at least match but ideally overmatch the threat posed by the use or threatened use of IEDs and can involve anything which is intended to predict, discover / detect, prevent, protect against, respond to / neutralize, recover / exploit, mitigate against, or deter IED attacks.

4 An assessment of the potential use of IEDs in a defined geographical area by stated IED threat actor(s) against stated target(s) in terms of the technical complexity and tactical sophistication along with the actor(s) intent, capabilities and opportunities along with local factors.

5 Often referred to as a 3C approach, this entails a policy approach that calls for engagements by C-IED donors to be coherent, coordinated and complementary. It seeks to consolidate whole of system approaches in trying to achieve a common goal.

6 An approach by all C-IED stakeholders including multiple elements of state security, defence, government departments and agencies and civil society organisations as well as international and regional organizations often with complex institutional structures and procedures to ensure internal coherence, a cooperative culture and collaborative efforts in support of an effective C-IED enterprise through a shared understanding of the assessed IED threat faced.

7 The term IED threat actor is a collective term for all persons, parties, groups, organisations and entities who have the intent and / or capacity to inflict or threaten physical violence through the use or threatened use of IEDs. IED threat actors can include both criminals as well as practitioners of irregular warfare which includes:

Terrorists	Partisans	Irregulars
Insurgents	Paramilitaries	Insurrectionists
Guerrillas	Fifth columnists	Saboteurs
Militia	Militants	Special forces
Subversives	Freedom fighters	

It is important to note that not all the terms listed as potential practitioners of irregular warfare use IEDs but they may use them as an asymmetric means to further their cause. Similarly, the designation of a group or actor under one of these terms may not be agreed by all commentators.

8 An IED system is the combination of people, processes and material that go into supporting, funding, procuring, manufacturing, transporting, targeting, preparing, emplacing, executing and publicising any element of an IED attack, including the indoctrination, training and life support of the persons involved.

9 IED network refers to the human elements of an IED system in terms of the personnel with the skills, knowledge, and competencies involved in any element of funding, procuring, manufacturing, transporting, targeting, preparing, emplacing, executing or publicising any element(s) of IED attacks, including indoctrination, training and life support of persons involved.

10 The specific design of an IED attack – including but not limited to position of the IED, the type of IED, method of actuation, intended target, type of road segment used, concealment technique, use of secondary devices, the time of day, etc. Tactical design addresses the questions of 'why here, why now, and why in this way.' Terms used to describe a specific type of device or component of a device (e.g., SVBIED, EFP, etc.) are often used to describe all or part of the tactical design.

11 Many methods of tracking IED tactical use are possible. For example, examining IED tactical use may track the IDREAD headings of Intended purpose; Delivery method; Role; Emplacement location; Attachment method; Device orientation.

12 US DoD. 2022. "Army C-IED Strategy." Washington DC: US DoD, February.

13 Chimp Reports, IGAD Chiefs Discuss Collaboration to Combat IED Threat. 02 Feb 22. Accessed April 23, 2022. https://chimpreports.com/igad-security-chiefs-discuss-collaboration-to-combat-improvised-explosive-devices-threat/.

14 IED exploitation is the process by which the parts of an IED system are recorded and analysed, to better understand such parts and the system as a whole. This will include analysis of the network(s); including threat actors, their roles and relationships; IED events; IED capabilities and associated IED components in use. It is important that exploitation activities are conducted persistently and iteratively to develop, maintain and sustain an accurate IED threat picture, to develop effective countermeasures and support the identification of network personnel, judicial processes and intelligence led operations. Exploitation activities will include collection and analysis of technical, tactical and forensic information. IED exploitation is an enabler that is required in attack / engage the network and defeat the device as it is a cross cutting process that transcends all aspects of a whole of system C-IED enterprise.

15 Alternatively the UNIDIR C-IED CMM SAT uses the broader term of 'engage the network.'

16 Such as the NATO system for evaluating collected items of intelligence.

17 This material has been adapted from MOSAIC 05.60, Border Control and Law Enforcement Cooperation 2012, Sections 6.3.1, 6.3.2, 6.3.3 and the WCO Annual Report 2022-2023 Pg. 59

18 This material has been adapted from https://www.interpol.int/Who-we-are/What-is-INTERPOL; MOSAIC 05.60, Border Control and Law Enforcement Cooperation. 2012. United Nations, Section 5.2; chemical-and-explosive-threats-interpol (gpwmd.com); https://www.interpol.int/Crimes/Terrorism/Chemical-and-Explosives-terrorism; https://www.interpol.int/Crimes/Terrorism/Chemical-and-Explosives-terrorism/Project-Watchmaker; UNIDIR Counter-IED Capability Maturity Model & Self-Assessment Tool, 2020 Pg. 24

ABOUT THE AUTHOR

Paul Amoroso is an explosive hazards specialist and has extensive experience as an IED Threat Mitigation Policy Advisor working in East and West Africa. He served in the Irish Army as an IED Disposal and CBRNe officer, up to MNT level, and has extensive tactical, operational, and strategic experience in Peacekeeping Operations in Africa and the Middle East. He has experience in the development of doctrine and policy and was one of the key contributors to the United Nations Improvised Explosive Device Disposal Standards and the United Nations Explosive Ordnance Disposal Military Unit Manual. He works at present in the MENA region on SALW control as well as in wider Africa advising on national and regional C-IED strategies. He has a MSc in Explosive Ordnance Engineering and an MA in Strategic Studies. He runs a consultancy, Assessed Mitigation Options (AMO), which provides advice and support in relation to conventional and improvised weapons and explosive hazard risk mitigation. This article reflects his own views and not necessarily those of any organisation he has worked for or with in developing these ideas.

Linkedin profile: https://www.linkedin.com/in/paul-amoroso-msc-ma-miexpe-60a63a42/