Tibor Horváth✧, Levente Tábi❖

Counter-Improvised Explosive Devices (C-IED) mission support capabilities

DOI 10.17047/HADTUD.2023.33.3.15

Actions and activities taken against the IED threat comprise complex tasks. In the beginning, the focus was on the deactivation and destruction of IEDs, as the only way to fight against them. As time has passed, more existing capabilities were included in the field of C-IED, which were able to contribute to the mitigation of the effectiveness of an IED attack.

Due to the fact that the first type of response to IED-threat was tasked to combat engineers, particularly to EOD personnel, that was rather obvious that C-IED missions and responsibilities fell to combat engineers. Nowadays, however, capabilities and capacities in the C-IED can be identified that exceed the competence of engineer units and commanders. The C-IED requires a comprehensive approach. In a staff and headquarters lots of capabilities and capacities should be involved in C-IED activities, which requires coordination and cooperation. The involvement of those capabilities depends on the type of mission, its phases, and the nature of IED threat. Thus a mission commander needs to understand which are the C-IED enablers that can contribute to C-IED tasks, when and how they influence or mitigate IED threats.

KEYWORDS: C-IED, Military Engineering, C-IED Enablers

Counter-Improvised Explosive Devices (C-IED) küldetéstámogató képességek

Az IED-k elleni tevékenység komplex feladat. A kezdeti időszakban még mindenki konkrétan az IED hatástalanítására, megsemmisítésére fókuszált. Az évek haladtával sorra jelentek meg az IED elleni tevékenységek során olyan, már korábban meglévő képességek, melyek hatékonyan tudtak hozzájárulni az IED támadások hatásfokának csökkentéséhez. Mivel a kezdeti időszakban az IED elleni feladatok kifejezetten a műszakiak, azon belül is a tűzszerészek

✧ University of Public Service, Faculty of Military Science and Officer Training – *Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar*;
E-mail: horvathtibor@uni-nke.hu; https://orcid.org/0000-0003-4742-847X

❖ University of Public Service, Doctoral School of Military Sciences – *Nemzeti Közszolgálati Egyetem, Hadtudományi Doktori Iskola;*
E-mail: tabi.levente@uni-nke.hu; https://orcid.org/0000-0003-0130-9248

feladata volt, így törvényszerűen a C-IED feladatrendszert a kezdeti időszakban a műszaki erők felelősségi körébe integrálták. Ma már viszont olyan képességek és feladatok is vannak a C-IED feladatai között, melyek már túlmutatnak a műszaki erők és parancsnokok kompetenciáján.

Az IED elleni tevékenység átfogó megközelítést igényel. Egy törzsben, parancsnokságban számos olyan képességet és kapacitást kell tudni bevonni a C-IED feladatokba, mely műveleti koordinációt és együttműködést igényel. A bevethető képességek a műveletek jellegétől, fázisaitól, illetve az IED veszély jellegétől függően vonhatók be. Így a műveleti parancsnoknak azt kell megértenie, hogy melyik képesség, mikor és hogyan tud hozzájárulni az IED által keltett veszély csökkentéséhez, esetleges megszüntetéséhez.

KULCSSZAVAK: *C-IED, Katonai műszaki, C-IED kiegészítő képességek*

1. Description of C-IED tasks

When introducing C-IED, we always start with defining an IED, the type of explosive materials we may encounter, and the nature of dangers presented. Without disputing the correctness of this approach, we wish to present C-IED tasks from the other side of the problem. According to the current interpretation of C-IED, an IED as a tool – in spite of the fact that it poses the greatest threat and takes a significant number of casualties – is not a top priority in NATO's C-IED approach. Today, it is the system, network and organization behind IEDs that NATO considers to be the most dangerous. Deactivating, restricting, or changing the conditions necessary for the operation of such organizations comprise a really important task and also the largest challenge.

C-IED tasks and the basic pillars of C-IED, have not changed. The same three determinants [attacking the network (AtN), defeating the device (DtD), and preparing the forces (PtF)][1] are used, which are based on the "Understand & Intelligence"[2]. The operational-level interpretation of these tasks is clearly defined in NATO's "Allied Joint Doctrine for Countering Improvised Explosive Devices" (AJP-3.15 (C)) C-IED doctrine[3]. The interrelations and priority of the three pillars mentioned above also depend to a large extent on the different operations and their individual phases. The priority of tasks in a peacekeeping mission is obviously different from that of a NATO Article 5 operation. The priority is also different when an IED emergency is not significant, and it is different if the threat significantly affects the success of operations. Therefore, a commander must always be aware of the nature of an IED threat and be able to determine exactly the extent, the means, and the way he intends to choose to deal with a particular IED emergency in order to reach the C-IED end state for the success of a particular operation.[4]

1 AtN, DtD, PtF – Tábi 2019, 179.

2 Understand & Intelligence – ibid.

3 NATO AJP-3.15 (C), Allied Joint Doctrine for Countering Improvised Explosive Devices. https://nso.nato.int/protected/nsdd/_CommonList.html.

4 Horváth 2016, 24.

2. The role and postition of the C-IED complementary capabilities

In the comprehensive approach of C-IED, it is essential for the successful execution of tasks to have the capabilities that, when applied together and in a coordinated manner, enable the achievement of the set goals. These capabilities are nothing more than the resources required to perform C-IED tasks in order to reach the C-IED end state specified by the commander. It is also important to clarify at the outset that there are only two units that can be labelled C-IED in NATO's interpretation. One is the so-called "Weapon Intelligence Team"[5] (WIT), which is officially referred to in NATO as "Level-1 Technical Exploitation", that is tactical level investigation team. The other unit is the "Level-2 Technical Exploitation", which comprises a criminal laboratory that can be installed in an area of operations and is capable, within certain limits, to analyse and evaluate the evidence collected in the area of operation. It should also be noted here right in the beginning that the development of these capabilities was based on real IED threats. Such units integrate the capabilities of other branches and special elements that are able to operate in other operational environments, in a completely independent fashion. Thus, for example, a conceptual WIT small unit is normally a four-member group (its composition also depends on the concrete nation, the operational situation, etc.), which represents the capabilities of reconnaissance, military operations, military police, and Explosive Ordnance Disposal.

As outlined above, in addition to engineers, C-IED tasks require other services, branches, and special elements as well, as they are capable of providing information and data that can be effectively used in C-IED tasks. Thus, if it is necessary to define "C-IED Enablers"[6], i.e. additional capabilities that contribute to C-IED tasks, then it is expedient to formulate it as "those resources and capabilities that are directly or indirectly capable of achieving the set C-IED goals, influence, contribute to or even carry out the tasks specified for the C-IED". These additional elements can be found in any operation, in their individual phases, and at all levels of military command (tactical, operational, strategic, and even political levels).

Therefore, looking only at the above stipulations, our statement that C-IED tasks have long been not only and exclusively the mission of engineer units and staffs can be well traced. Moreover, in the later analysis it will be presented that the comprehensive approach to C-IED tasks is not dominated by engineer subunits and special tasks, but rather by reconnaissance and operational cooperation, which will bring the expected and determined success.[7] In order to support this statement, we now examine the C-IED complementary capabilities and the way they can contribute to the end state defined by the commander.

---

5 Weapon Intelligence Team – NATO C-IED Field Exploitation (Level-1) (tactical-level NATO crime scene investigation team, also called WIT – (AJP-3.15 (C), 2–9; 49.)

6 C-IED Enablers – (AJP-3.15 (C), 1–16; 34.)

7 Horváth 2019.

3. Additional skills and the objectives to be achieved through them

The comprehensive approach to C-IED also requires that the available forces be able to support C-IED tasks and contribute to the expected success based on their primary assignment. In all five services of NATO (land, air, naval, special operations, and cyber), there are forces, capabilities, and sub-capabilities that can affect C-IED missions.

In accordance with its definition, an IED is basically a tactical weapon that can achieve strategic effects,[8] therefore under normal circumstances, individual tactical level capabilities in the C-IED environment can have a significant impact on the objectives set at higher leadership levels. Therefore, each capability is interpreted on the basis of the level of their added value to the C-IED objectives and not according to the deployed capabilities. Priority is irrelevant here, as it has previously been interpreted, because according to the phases of operations, priorities change, may change, or the operations themselves induce different needs in different IED emergencies.

3.1. Patrolling

First, let us look on the patrol as a basic combat unit. Although this is not a specific capability, it may play a decisive role in operations.

The unit assigned to such a fundamental operational task can be a very important sensor for a staff coordinating C-IED missions. A commander deploys patrols for various purposes and tasks (e.g. demonstrating the presence of forces, escorting convoys, ensuring the movement of protected persons, etc.). It is not included in the basic function of a patrol to take an action against an IED system, however, in most of the cases these are the units that suffer the most IED attacks. Therefore, patrols, when moving in an IED-infested operational environment, need not only to be prepared for the proper response to a particular IED attack, but they must also be enabled to notice the signals, responses, and reactions before an IED attack could occur. In other words, a well-prepared patrol can provide basic information to staffs and commands about what is happening in the area of operations without even specific IED attacks taking place.

3.2. Military Search – MilSearch[9]

Military Search was established in connection with C-IED missions. It should in no way be confused with the Air Search and Rescue Team, which is operated in accordance with international standards, for example, as a standby force maintained

8 See the 2004 attacks at the Madrid railways resulting in the withdrawal of the Spanish forces from Iraq, or the exponential developments of the EOD capabilities in the HDF in 2008-09, induced by the cases of Hungarian EOD troops killed in action in Afghanistan in 2008.

9 Military Search – Systemic operation by land forces aimed to allow the unit commander to ascertain if an object, person, information is located in a place and at a time. NSO, The Official NATO Terminology Database: https://nso.nato.int/natoterm/Web.mvc

by the Air Force within the Hungarian Armed Forces. Military Search is an explicite ground operation (even if the forces deployed in the depth may be inserted by air). In the framework of MilSearch, a specific objective or area is monitored, reconnoitred, or searched by specially trained personnel in order to provide the commander who gave the task with certainty and confirmation that the persons, materials, objects, or equipment sought or suspected are present at the location under surveillance, or what events are taking place at the observed location. In dependence on the location of a target area or target object – for example, how dangerous it is to move within a given area and to what extent it is necessary to involve a specialized professional team to find the objects sought – the composition of the MilSearch Team may change significantly. Since the development of Military Search can be linked to IEDs, the creation and construction of this type of operation was initiated by the engineer forces (by EOD specialists). However, in the course of capability development, it is not only engineers who are in these groups, but also combined-arms forces or special operations forces for various security tasks. If a host nation[10] has the appropriate capabilities, then involving them is not only advisable but also recommended. However, if operations take place on their own national territories or on the territory of a NATO ally, the involvement of local, national law enforcement and security agencies must be explicitly taken into consideration. Consequently, the specific search operations can be planned and organized by engineer units, but the planning of the entire operation also requires the preliminary collection and processing of intelligence, and the planning, organizing, and directing functions of the operation. Depending on the level of emergency in the given area (not only on the IED threat but also on risks generated by enemy forces) and the level of profession-specific research teams to be deployed in the area, NATO determines three levels of military search teams. The basic search group is capable of performing a task with a large number of people at a low level of emergency, at middle level with the risk increasing the number of troops in the group decreases, while the highest level team is a specially trained small unit operating in a high-emergency environment.

3.3 Route Clearance[11]

Another task specifically accounted for as an engineer capability is the capability of "Route Clearance" in an IED-infested environment. This is basically an engineer reconnaissance mission performed on a given route, which usually involves the additional task of the deactivation of any explosive device discovered. Therefore, there are many factors to consider during the execution of such a mission. The composition and capabilities of the unit assigned to the task determine a number of planning criteria. In accordance with NATO's Route Clearance Concept, four levels need to be distinguished in terms of capabilities and capacities. These levels differ fundamentally in their equipment and mobility. The first level is a fully dismounted

10 Generally abbreviated as HN.

11 Integrált Terminológiai Adatbázis, 2019, NATOTerm, line 3475.

route-clearing unit conducting its mission manually, while the fourth level is a completely mechanized convoy equipped with state-of-the-art technology. Units of the fourth level include armoured machines performing the special tasks, combined-arms forces covering them, as well as a logistic element providing combat service support.

Time factor is paramount in such missions as regardless of the executive levels, this task is extremely time consuming. Finding and locating an installed explosive device, even with the use of advanced, mechanized, digital devices, take a considerable amount of time, not to mention the deactivation of the discovered explosive devices and the clean-up of that route section. However, it should also be taken into account that the cleared route can only be labelled secure for a certain period of time after the completion of demining by the unit. As early as the planning of a route clearence operation it is necessary to define how long the so called "time window" should be, how long a road section should be secure, free to use, and when it can be forecast that another IED may be re-planted on that particular road section, making it dangerous to our own maneuvers or completely unusable again.

During NATO's ISAF operations, the Air Force was also deployed for so-called "Route-Burning" operations. This meant that an airplane with special equipment flew along a designated route, blocking and limiting the usability of the radio-controlled explosive devices on the route. This solution is efficient if it targets radio-controlled improvised explosive devices that are typical for a given area of operations. However, it must be understood that the time window mentioned above restricts freedom of movement in such cases as well. Furthermore, in order to apply this method of route clearence, it is necessary to know the frequency at which signals must be emitted in order to detonate a given explosive device and to declare a given route secure and demined.

A "Route Clearance" capability should be assessed on the basis of the success of C-IED tasks. According to some unofficial sources, the ability of the highly modernized and mechanized "Route Clearance" package in ISAF C-IED operations could contribute barely 20% to the success of the fight against IED. Therefore, it has to be seen that IED problems cannot be solved by this capability alone. The Route Clearance capability remains a response to IED threat rather than a proactive action.

3.4 Explosive Ordnance Disposal and Improvised Explosive Device Disposal missions (EOD / IEDD)

When conducting actions countering IEDs, Explosive Ordnance Disposal troops provide a very special capability. EOD personnel are tasked basically with search for and deactivation of bombs, missiles, ammunition, etc. left over from fighting, which means they carry out the clearance of the area. From this principle it follows that no other than EOD personnel are the trained soldiers who are capable of deactivating even improvised explosive devices. As a result, nowadays the missions of an EOD unit are not limited exclusively to the deactivation of dangerous devices left over from armed conflicts, but also IEDs of any kind. However, what does that mean in reality?

First of all, not all EOD personnel are trained and prepared to disarm or manipulate an IED. In the armed forces of certain NATO nations, for instance in the HDF, classic EOD missions are clearly separated from IED deactivation tasks. In other nations, these organically different tasks are integrated almost inseparably. Therefore, in dependence on the nations involved in the cooperation, it is necessary to clarify exactly the particular limits and limitations of each national capability, because this will determine who can be assigned to and involved in what task.

A new expected capability for EOD personnel is to actively perform tasks in the WIT – "crime scene investigation team"[12] or possibly in the MILSearch unit. When conducting WIT tasks, the EOD are expected not only to neutralise a discovered IED but also to gather evidence related to the explosive device on site after the explosion. They are required to analyse the IED event as well as the primary evidence from a professional aspect, and then evaluate the incident and the explosive device itself from tactical and technical points of view.

If EOD personnel are capable of gathering appropriate evidence from the scene and draw the appropriate professional conclusions from it, they can greatly contribute to further evidence analysis, as well as draw attention to the attack pattern of IED users or the threat posed by a newly developed and deployed IED. This is why it is very important for EOD experts not only to recognize an IED as a tool, but also to be able to analyse it, both for force protection purposes and for facilitating activities countering IED.

3.5 Military Working Dogs[13]

The use of military working dogs has multiplied the capability and efficiency of C-IED missions. Along with its trainer a well-trained working dog prepared to search for IEDs do outstandingly productive work and can provide security to the units performing operational tasks. However, the presence of a working dog in EOD unit does not mean automatically that it is 100% able to perform C-IED tasks.

Working dogs are only prepared for one particular task. Therefore, a dog that has been trained to search for drugs, for example, will not be able to identify explosives; or a working dog trained to detect antipersonnel minefields, for example, will not recognize a planted IED. Therefore, it is very important that the commander and the staff of the operation were exactly aware of the operational abilities and limitations of a particular dog before ordering it to any job at an operation. That is why it is expected and determined that working dogs must also be tested and qualified before they can be deployed to a real task.

Another important factor for the use of working dogs is the limitations of the dogs. The sex, age, and breed of the dog clearly limits certain abilities. In operational tasks, a working dog and its trainer, its "owner", must be treated as a pair; one without the other will not be effective.[14]

---

12 See at point 3.7 C-IED - C-IED Exploitation.

13 AMWDP-1, Military Working Dog (MWD) Capabilities, point 5, 14.

14 In PPT presentation "Jelentések struktúrája, C-IED COE: C-IED Enablers", slide 14.

3.6 Information Operations[15]

An Information Operation (IO), similarly to C-IED operations, is a very complex, multi-player mission. It is a complex staff function, which includes the analysis, planning, and evaluation of the acquired data and information, as well as the integration and coordination of the necessary activities. Based on its content, an Information Operation is nothing more than the determination of the effects to achieve in the designated target audience, in line with the commander's intent. From NATO's aspect, IOs can be divided into two basic levels: strategic-political level, which is usually called STRATCOM[16]. This basically means diplomatic (political) communication as well as informing the public. The other level, which is clearly subordinated to STRATCOM, is INFO OPS itself, which is much more of an activity in support of military operations.

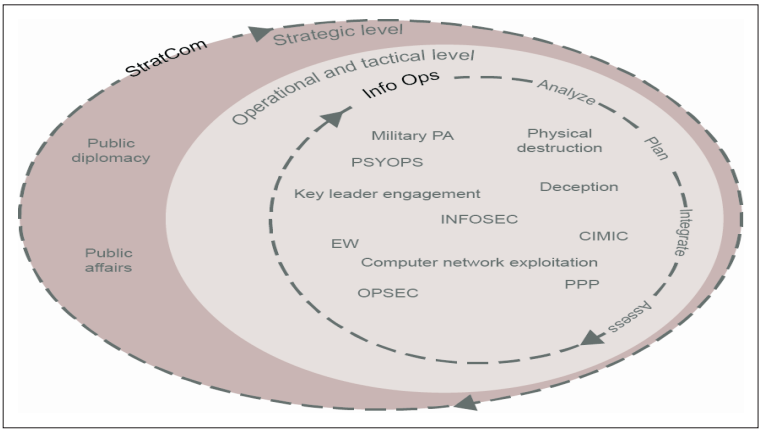

Figure 1.
STRATCOM – INFO OPS system
(AJP-3.10, Allied Joint Doctrine for Information Operations, [Figure 1.3, Page 1–20] 34.)

INFO OPS, as shown in Figure 1, comprise not an exclusively communication activity. They have a number of elements that the C-IED may use only indirectly or not at all. However, there are INFO OPS elements that can specifically contribute to the achievement of C-IED objectives. From a C-IED perspective, there are only a few partial INFO OPS activities that can have a concrete impact on the success of C-IED tasks.

The so-called "Key Leader Engagement" (KLE)[17] is a very important element of the comprehensive approach to C-IED. This means nothing more than conducting

15 AJP-3.10, Allied Joint Doctrine for Information Operations.

16 STRATCOM – Strategic Level Communication, AJP-3.10, Allied Joint Doctrine for Information Operations, (0104. Page 1–3) 17.

17 KLE – Key Leader Engagement – cooperation, coordination, discussion with and occasionally oriented preparation of leaders (as interpreted by the authors based on C-IED missions), AJP-3.10, Allied Joint Doctrine for Information Operations, (0135. Page 1–14) 28.

forums (conferences, seminars, workshops, etc.) for responsible political and military leaders, where IED as a basic problem and C-IED as a solution can be discussed. In addition, the KLE provides an opportunity, especially within the national framework, for the representatives of various armed forces and law enforcement agencies to coordinate national C-IED capabilities and missions.

INFO OPS have a very important role in the appropriate information of the public. Of course, it should also be remembered that this means not only providing information – especially not in a hostile area of operations – but also influencing the local population (PSYOPS)[18] through proper communication. However, before any negative interpretation of the above, on a doctrinal basis, from a military and operational point of view it needs to be clarified that, according to the operation commander's intent and decision, PSYOPS should be used to inform the civil population to an extent that the population did not impede the success of operations. Perhaps it is even more important to achieve with proper communication of C-IED tasks the prevention of the public from supporting the forces and groups that intend to use IEDs. So positive information and influence, as well as the use of proper communication for tuning the public against hostile groups can all be a suitable tool to achieve C-IED goals.

In accordance with NATO's approach, Electronic Warfare (EW)[19] is part of the IO. Merely a few years ago, Electronic Warfare was regarded an explicit military operation. However, with the advancement of cyberspace and the development of the digital world, EW also became increasingly open from the military to the civil sector. EW monitors and manages activities in the entire electromagnetic spectrum in current sense of the word. It performs all these missions, in a military sense, from tactical to strategic level.

In terms of C-IED, in the electromagnetic spectrum EW tasks are to be performed essentially for the purpose of determining, detecting, reducing, or preventing an IED network from using the electromagnetic spectrum effectively.[20] At the beginning of the development of C-IED missions, it was very important to have adequate electronic protection for friendly units conducting tasks in the area of operations where explosive devices were typically operated through radio control. Therefore, radio frequency jammers were first developed and introduced in a protective manner in order to provide radio frequency protection. The primary function of these devices was to suppress all electromagnetic signals in a pre-set frequency range, thus preventing radio-controlled explosive devices from being activated. At the same time, however, it was important to be able to maintain operational communication during all this time. That is why the EW personnel was needed who knew which frequencies to keep for communication and which to jam. It should be noted here that even with such electronic jamming, it was not possible to cover the entire electromagnetic spectrum. Thus, reconnaissance and scientific analyses played a major role in determining the range of radio frequency in which the opposing parties intended to operate their radio-controlled devices.

18 PSYOPS – Psychological Operations.

19 AJP-3.6, Allied Joint Doctrine for Electronic Warfare. (Chapter 1, 21–23.)

20 AJP-3.6, Allied Joint Doctrine for Electronic Warfare. (Chapter 1, 21–23.)

Later, mainly due to the appearance of more sophisticated enemy assets, it was no longer enough to just maintain a defensive position in EW missions. It was necessary to move forward and establish a proactive posture in the execution of EW missions in order to enable NATO and its allies to take more effective actions against IED networks and IED systems.

Therefore, it is relatively easy to identify which C-IED pillar the EW can support and in what way. AtN, for example, may be supported by EW reconnaissance, gathering digital information, and providing databases, or directly intercepting the communication of target people. In the case of DtD, for example, the execution of tasks related to electronic jamming, while in the field of PtF, it is the organization of training programs related to the management of specialized equipment and the implementation of projects aimed at raising awareness to radio-controlled explosive devices that comprise the responsibilities of EW.

3.7 C-IED Exploitation[21]

Appropriate analysis of scene and evidence collected on site with advanced tools of science and technology is a critical capability in C-IED operations, including activities against an IED network. NATO distinguishes at least three levels in this capability.

The first level is a tactical level detection team – the equivalent of a police crime scene investigation team. In NATO, this operations group is called "Weapon Intelligence Team" – WIT[22]. The specific composition and strength of teams depends on the particular operation, the IED threat, and the capabilities available as well.

For the WIT, conceptually, a four-strong group is taken as a starting point, which includes an EOD expert who can professionally analyse the given improvised explosive device (IED) or its remains; an operations specialist who analyses and evaluates the performance of his own team; a reconnaissance specialist who analyses and evaluates the enemy/insurgents' combat procedures; and finally it is advisable to have a Military Police Officer/Provost Marshal in the team, to represent the rule of law in order to make the collection of evidence by WIT and their analysis legally acceptable in court proceedings. Therefore, the most important task of this team is to gather evidence and information from the scene (about the IED, the methods of execution, possible perpetrators, and the actions taken by friendly troops) and then forward them to the appropriate authorities, with a professional analysis attached.

The evidences gathered by WIT are taken to the next level, which is called Level-2 Technical Exploitation, a laboratory that can be deployed on the battlefield. This type of laboratory can be installed in the area of operations or, depending on its equipment, can perform additional analyses of the evidence collected from the scene. This includes professionals who are able to produce concrete findings about an evidence on a scientific basis using special instruments and procedures. These clues may be fingerprints or DNA analyses, interception of radio traffic or retrieval

21 AIntP-10, Technical Exploitation, Chapter 2, 15–17.

22 WIT (Weapon intelligence Team) – NATO Field Exploitation (Level-1) tactical-level NATO crime scene investigation capability) – (AJP-3.15 (C), 2–9; 49.)

of media data from telephones, or even the identification of explosive components. All of this information is important in order to narrow the scope of an investigative activity to individual perpetrators, as well as to make them useful in particular criminal proceedings. However, such laboratories do not always have the investigative capabilities necessary for a full-scale analysis in all areas of operations. Therefore, NATO has defined a third level of evidence analysis, which may be a national forensic laboratory established and operated outside the area of operations.

In such a forensic laboratory, depending of course on the capabilities of the laboratory set up by a given country, it is possible to carry out various analyses of the collected and delivered evidences in a fundamentally complete spectrum. At this level, it is already possible to identify the perpetrators on the basis of evidences and existing databases, and to make proposals for reviewing certain combat procedures, for considering new acquisitions, etc., or expert analyses for criminal proceedings can also be provided based on the findings.

The three levels are built on each other and complement each other. Each level prepares reports based on its analyses, which are always sent to the relevant persons.

The real benefit of the ability to spot and analyse evidence is that the evidence and information gathered from an area of operations is analysed with due professionalism, and if every stage of the procedure is properly performed, all evidences can be used in a prosecution. So not only can the information extracted be used to identify a perpetrator, but also to legally sanction those involved in the crime.

However, it is important to emphasize here that this three-tier capability that complements C-IED missions, is no longer a purely military-based capability. Depending on the nation, each member state has different capabilities and capacities. Moreover, it is typical that a third-level national laboratory does not operate under

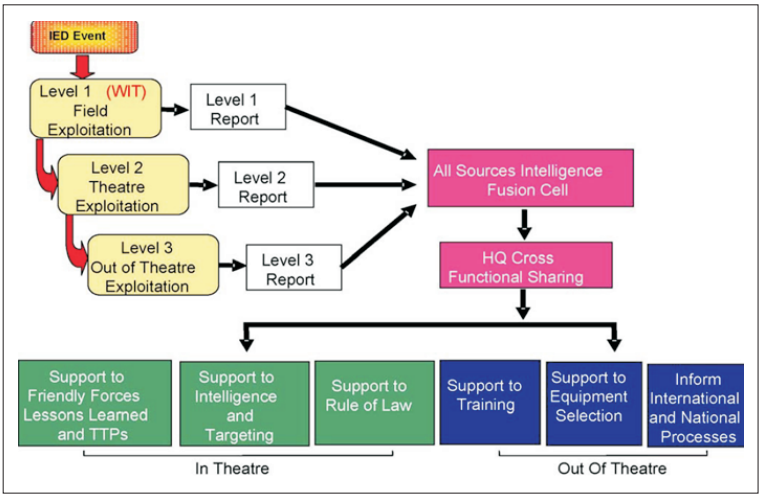

Figure 2.
Structure of the evidence analysis reporting system
(PPT presentation „Jelentések struktúrája, C-IED COE: C-IED Enablers", slide 29.)

the supervision of the army, so before the beginning of operational tasks – or during the procedure – cooperation must be established between the parties involved, which may even be international.

The evidence and information gathered can also be analysed from another perspective. Some developed countries have established and operated research institutes where various IED events and their details are examined and modelled through scientific (mathematical) analysis. As a result, hot-spots[23] can be identified for an area of operations, and the location, possible time, and/or nature of the next IED attacks can be predicted with relative precision.

3.8 Biometrics[24]

Biometric analysis provided a new opportunity to identify the population living in the area of operation. It is a well-known fact that a person can be clearly identified with the use of three methods, as there are unique features that can only and exclusively be linked to one person.

It has been long known about fingerprints and DNA that a person can be clearly identified with them. However, for the analysis of these factors, the collected samples must be tested under laboratory conditions. These laboratory tests primarily determine the unique identifiers of the samples only. If a sample of a person is not stored in the central database, or there is no control sample that can be linked to a specific person, then the laboratory test will not be sufficient to support a criminal proceeding.

This is where the collection and analysis of biometric data can be a great help. Now it is known that in addition to DNA and fingerprints, the iris of the eye is just as unique as the previous two. However, one of the advantages of iris testing is that it does not require laboratory testing to identify the individual, so there are no significant time factors or financial resources involved. The establishment of an appropriate database and checking the biometric data of an individual allow for a nearly instant identification of a person even in an area of operations.

However, it should also be taken into consideration that biometric data alone are not sufficient for a possible subsequent court proceeding. For this, the evidence must be linked to the individual, which can be achieved with a positive result from DNA and fingerprint tests. The two analysis systems are thus able to complement each other, provided that the relevant data are collected and stored in a central database and are constantly updated.

3.9 Air and Space Warfare

At first, perhaps during NATO's operations in Afghanistan, it was felt how effective role the Air Force could play in C-IED missions. With the development of technology,

23 Hot-spot: areas, geographical regions where most of the IED events take place.

24 Biometrics: – Automated recognition of individuals based on their behavioural and biological characteristics, NATO AJP-3.15 (C), Allied Joint Doctrine for Countering Improvised Explosive Devices, Part 2 – Terms and definitions, LEX4, 100.

the specialization of tasks, and the transformation of the capabilities and combat procedures of the opposing forces, the air force has also undergone a significant transformation in terms of C-IED tasks.

While at the beginning of operations the air force was able to offer its speed, fundamentally unrestricted mobility, and precision attack capability to support the achievement of C-IED objectives, it is now able to provide unmanned aerial systems and space warfare potentials for C-IED missions in a variety of ways. The wide range of aerial reconnaissance and strike capabilities contributes significantly to the efficient and effective execution of C-IED operations and tasks.

Naturally, the capacity provided by drones is also used by opponents, so now this threat is a new challenge for the air force as well, because while it was involved in offensive operations for a very long time, nowadays it has to implement significant defensive rules to continue in order to maintain control of the airspace of operations.

3.10 Naval operations

Under normal circumstances, it would be reasonable to think that a navy would participate in C-IED tasks only if there was a naval base in the area of operations that needed protection or if Allied warships were threatened by IED attacks. This is basically true, but like everything else in the development of C-IED the Navy has also progressed, evolved, and integrated into unified C-IED missions for common success.

At present, a navy is capable of the participation in C-IED missions almost with its entire arsenal. Thus, naval bases are not only protected against IED attacks, but can also accommodate even "Level-2" laboratories. In addition to ship defence, the naval electronic capabilities now conduct monitoring, interception, and evaluation, and provide data not only on targets moving on water but also on land. On the water the navy plays a very important role in the tasks against IED networks. Not only does it intercept ships under embargo, but based on appropriate intelligence, it is also capable of carrying out land-based "Intermediate Search"[25] on ships, vessels and platforms in international waters with the use of so-called "Boarding Team"[26].

In light of all this, however, it must be seen that similarly to IED systems[27] a C-IED task force is able to perform its missions far away from its specific area of operation. In other words, the international trade in IED systems, which has been well coordinated so far, can be effectively influenced and limited by integrating naval capabilities for C-IED purposes.

---

25 Intermediate Search –ATP-3.12.1.1, Allied Tactical Doctrine for Military Search, Chapter 3 - Search Capability 0304. 3–1 page, 23.

26 Boarding Team – NATO ATP-71 Allied Maritime Interdiction Operations, 0107 Definition of Key Terms, point s. Boarding Party1–5; 25.

27 IED system – the personnel, resources and activities necessary to resource, plan, execute and exploit an IED event. NATO AJP-3.15 (C), Allied Joint Doctrine for Countering Improvised Explosive Devices, Section 2 – The IED system Section 3 – The C-IED Approach, 1-2 page, 20.

3.11 Secret services

It is an open secret that secret services usually have diverse intelligence collected from open sources or classified sources, in dependence on their capabilities and the complexity of the particular security situation. Consequently, from a "user's" point of view, there is a need in the case of an IED emergency for the capability of retrieving such intelligence, or for sharing and processing the intelligence in cooperation with security agencies.

This is a two-way street. All stakeholders need to know what steps need to be taken towards each other in order to effectively achieve the common goal of reducing and eliminating IED threats.

3.12 Host Nation Support and local population

It is well known that it is the community living in its own microenvironment that knows best all the events taking place there. In any case, they are the ones who can make the most authentic statement about what is happening and they know exactly who did what, when, and where in their environment, community. That is why it is important for the national security agencies of a country to maintain good relationships with the population. It may seem similar to the stories about Hungarian King Matthias the Just that, for example, in Jordan the population has an extremely high level of trust in the King of Jordan and the governing forces he leads, as a result there is an excellent and reliable relationship between local communities and security forces.[28]

It is also a well-known fact that on the battlefield of the Balkans, it was the local population whose assistance allowed for mapping the location of various minefields and explosive obstacles installed during the fighting. The same fact is confirmed by the lessons learned from operations in Afghanistan and Iraq, where the losses of Allied troops significantly reduced thanks to good relations with the local population and security forces.

Of course, there are also other benefits stemming from cooperation between forces involved in a classic peace support operation and the local bodies operating in the area than those between Allied forces and the Host Nation Support provided by a member state during a NATO Article 5 operation.

You always need to know exactly what support can be requested from and be provided by a host nation. It is equally necessary to know the existing cooperation regulations of the allied forces and the domestic security bodies, who has what role and room for manoeuvre in an action against an IED network/system.

Based on the above, it can be seen that local communities have a very important role to play in the struggle against IED threat. If residents are vigilant, "keep an open eye" for their environment, and pay due attention to events in their community, they can provide very important and accurate information to security forces if there

28 Tábi 2019.

is an appropriate network of contacts. This is why it is important for the population to have confidence in the security forces and to provide data on local anomalies on a permanent basis.

This also refers to the relationship between the local security agencies, forces that provide Host Nation Support, and the allied forces that carry out their operations. Sharing information in a timely manner is as important for all concerned parties as carrying out joint operations, supporting and complementing each other's tasks.

4. Tasks of a C-IED staff with additional capabilities

As mentioned above, in its own way each task is able to support both C-IED missions and the commander's intent, and to help achieve the desired end state. However, it should also be seen that these tasks alone are not sufficient to achieve the set results or end state. These complementary capabilities may work effectively in their own operational environment, however, in a C-IED environment it is quite possible that a need arises for more than just such professional activities. A good example is the RC capability[29], which was much less efficient than expected on the basis of the millions of dollars invested in it. Or what is the point in a successful raid by Special Operations Forces if they are unable to gather the requested evidence or there is nobody to analyse it with the use of appropriate methods? The list of such examples would be long but the point is the same: for C-IED, all of these capabilities and tasks need to be coordinated.[30]

In our opinion, only a well-trained staff is capable of conducting such a comprehensive mission. Collected intelligence is analysed by intelligence officers, but only a team trained in the field of C-IED can filter out an IED network[31] from the many other networks in the field. EW personnel can tune in all frequencies, but it is the C-IED staff that can provide information on the frequency to be monitored, jammed, etc. in a given operation.

Thus, in the course of action against an IED network, an IED system, or an explosive device, coordination, proper sharing of information and processing in terms of C-IED are essential. A C-IED staff and its specialist personnel must know exactly what capabilities are available or requestable and the possible operational limitations they may have. With these factors in mind, operations need to be planned, organized, and managed. Of course, the entire planning of operations will not be be taken over by the C-IED staff, but it can have an impact on mission planning that can positively affect the success of C-IED tasks.

29 RC – Route Clearence, see point 3.3.

30 Horváth 2014.

31 IED hálózat – interconnected human and/or material nodes that may be identified, isolated or engaged. NATO AJP-3.15 (C), Allied Joint Doctrine for Countering Improvised Explosive Devices, Section 3 – The C-IED Approach, 1-5 page, 23.

Conclusions

The complexity of C-IED tasks does not stem from the fact that complex calculations and complex plans have to be prepared, but from the fact that they require extensive, continuous, and multi-directional coordination and communication from all participants. In addition to all these, it also requires adequate preparedness as the IED threat and the IED system keep constantly changing and transforming. Parallel with the advances of technology, IED makers are able to produce increasingly modern and efficient explosive devices, and IED networks also utilise up-to-date networking methodologies.

That is why development in the area of C-IED has to be maintained and it should not get focused only on neutralising an IED as a tool. There are several ways to reach an end goal set for C-IED. Capabilities from different professional areas can be involved and applied for this. But these capabilities, even if they successfully perform their tasks in their own fields, can effectively support and facilitate the C-IED end state only if there is proper coordination and communication within the given staff.

It should also be clarified that not all of the requestable capabilities need to be employed at once, just because a mission is to be executed in an IED-infested environment. The C-IED staff element (whether it is only one person, a small team, or a complex staff section) must continuously assess the current IED threat, and involve only skills in the planning and execution of missions that can contribute to the effective realization of C-IED tasks.

The objective of this study is to present a set of skills appearing in the relationship of C-IED tasks, which usually work effectively in their own professional approach. Here we attempted to gather all the additional capabilities associated with C-IED tasks that, to the best of our present knowledge, may contribute to the success of C-IED actions. In the study, the emergence of individual abilities is not a priority. Moreover, it was clearly emphasised from the beginning that the priority of the application of missions and skills is influenced by many factors that must be accurately mapped, analysed, and evaluated. It will only be possible to determine as a result of such a complex procedure to what extent this complementary capability can effectively support C-IED missions in a particular situation. There is no 100%-certain golden rule in this system apart from the principles of common sense, logical thinking, and open communication.

BIBLIOGRAPHY

AAP-15 (2017–2018). NATO Glossary of Abbreviations used in NATO documents and publications. Source: file:///C:/Users/CoeUser/Downloads/AAP-15(2017-2018)%20EF.pdf, (Downloaded: 28. 02. 2019.)

AIntP-10 2015. Technical Exploitation. Edition A Version 1, September 2015. Source: https://nso.nato.int/protected/nsdd/_CommonList.html (Downloaded: 17. 11. 2020.)

AJP 3.15 (C). 2018. Allied Joint Doctrine for Countering Improvised Explosive Devices, Edition C Version 1, February 2018. Source: https://nso.nato.int/protected/nsdd/_CommonList.html (Downloaded: 04.03.2018.)

AJP-3.10. 2020. Allied Joint Doctrine for Information Operations. Edition A Version 1, December 2015. Source: https://nso.nato.int/protected/nsdd/_CommonList.html (Downloaded: 17. 11. 2020.)

AJP-3.6,. 2020. Allied Joint Doctrine for Electronic Warfare. Edition C Version 1, March 2020, Source: https://nso.nato.int/protected/nsdd/_CommonList.html (Downloaded: 17. 11. 2020.)

AMWDP-1 2018. Military Working Dog (MWD) Capabilities. Edition B, Version 1, May 2018, Source: https://nso.nato.int/protected/nsdd/_CommonList.html (Downloaded: 17. 11. 2020.)

ATP-3.12.1.1. 2017. Allied Tactical Doctrine for Military Search. Edition C Version 1, October 2017. Source: https://nso.nato.int/protected/nsdd/_CommonList.html (Downloaded: 19. 11. 2020.)

ATP-71. 2020. Allied Maritime Interdiction Operations. Edition B Version 1, Ratification Draft/June. Source: https://nso.nato.int/protected/nsdd/_CommonList.html (Downloaded: 19. 11. 2020.)

C-IED COE*: „C-IED Enablers",* ppt előadás, 2018. október, a NATO SPS: „Comprehensive Package for strengthening Jordanian C-IED defence capabilities, 2017-2018" projekt során levezetett „C-IED Awareness Course" tanfolyam anyaga, a szerző átdolgozásában

Horváth Tibor 2014. Az ISAF Északi Regionális Parancsnokság felépítése, törzse és működése. In: Boldizsár, Gábor; Wagner, Péter (szerk.): *A Magyar Honvédség befejezett szárazföldi műveletei Afganisztánban – Tapasztalatgyűjtemény.* 67–72. Budapest: Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar.

Horváth, Tibor 2016. Az IED hálózat, mint korunk egyik aszimmetrikus kihívása. In: Csengeri, János; Krajnc, Zoltán (szerk.): *Humánvédelem – békeműveleti és veszélyhelyzet-kezelési eljárások fejlesztése.* 275–298. Budapest: Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar.

Horváth Tibor 2019. Emergency cases at countering improvised explosive devices, and their potential management. *Revista Academiei Fortelor Terestre / Land Forces Academy Review,* 94: (2): 95–106. https://doi.org/10.2478/raft-2019-0011

MH TP, *Integrált Terminológiai Adatbázis*, 2020. 09. 28. Forrás/Source: http://mhkdab/$table:SYS.VIEW.%C3%96SSZES.TERMINOL %C3%93GIA.TERMINOL%C3%93GIAI%20ADATB%C3%81ZIS)

NATO AJP-3.15 (C), Allied Joint Doctrine for Countering Improvised Explosive Devices. https://nso.nato.int/protected/nsdd/_CommonList.html.

NATO Standardization Office, The Official NATO Terminology Database. Forrás/Source: https://nso.nato.int/natoterm/Web.mvc (Downloaded: 17. 04. 2019.)

Tábi Levente. 2019a. A nemzetbiztonsági szolgálatok és fegyveres szervek együttműködésének tanulságai. *Szakmai Szemle,* XVII (4): 178–189.

Tábi Levente 2019b. *Comprehensive Package for strengthening Jordanian C-IED defence capabilities*. Springer Link.