Christopher Young

DOI:10.33179/BSV.99.SVI.11.CMC.24.2.2

NAČRTOVANJE ZA USPEH: POZIV K OPTIMIZACIJI KIBERNETSKEGA USPOSABLJANJA V OKVIRU NATA

PLANNING FOR SUCCESS: A CALL TO OPTIMIZE NATO CYBER TRAINING

Povzetek Usposabljanje je naložba v jutrišnji dan, ki jo spodbujajo današnje potrebe in viri. Pravilno oblikovanje usposabljanja je zamudno, še zamudneje pa je, če ga izvedemo slabo. Model, ki ga Nato uporablja za oblikovanje in evalvacijo svojih programov usposabljanja, temelji na sprejetih področnih standardih, vendar pa se v okviru kibernetskega prostora ne uporablja nujno v celoti. Učinkovitost modela je odvisna od objektivne kakovosti rezultatov, ki jih ustvari, vendar so razvojne pobude pogosto prenagljene ali premalo podprte. Tudi sedanje evalvacijske prakse ne potrjujejo dovolj kakovosti pripravljenega usposabljanja. Načrtovanje mora biti skrbnejše in bolj premišljeno, da se oblikujejo dobre rešitve v kibernetskem usposabljanju za zavezništvo in zagotovi doseganje organizacijskih ciljev.

Ključne besede *Model ADDIE, učinkovitost usposabljanja, vrednotenje, Kirkpatrickov model.*

Abstract Training is an investment in tomorrow fueled by the needs and resources of today. It is time-consuming to build training correctly, but even more so to do it poorly. The model that NATO uses to create and evaluate its training programmes is based on accepted industry standards, but it is not necessarily being used to its full potential in the area of cyberspace. The efficacy of the model is predicated on the objective quality of the deliverables it produces, yet development initiatives are often rushed or under-supported. Current evaluative practices also do not sufficiently confirm the quality of the training produced. More careful and deliberate planning is required, not only to create valid cyber training solutions for the Alliance, but also to ensure that its cyber training achieves organizational goals.

Key words *ADDIE Model, training efficacy, evaluation, Kirkpatrick Model.*

Introduction

Like any large organization, NATO has at its disposal many options for achieving its strategic goals in cyberspace. Policies can specify tasks and measures of quality, or programs can help simplify workflow, improve communication and manage resources. A tool NATO frequently relies upon to effect changes in human behavior is Education and Individual Training (E&IT). While highly valued by the Alliance, training can be costly to implement and maintain. In 2015, it was estimated that 356 billion was spent globally on corporate E&IT ventures (Beer et al., 2016, p 3). A 2010 Chapman Alliance analysis provides some granularity on the cost, suggesting that, on average, companies spent nearly 6,000 per hour to create instructor-led E&IT and just shy of 10,000 to create one hour of e-Learning E&IT (Chapman, 2010). While somewhat dated, the Chapman study helps to provide an appreciation of the magnitude of the cost behind creating training.

Considering the high cost associated with training, how significant of a return on investment is NATO recognizing for its cyber E&IT ventures? The only way to know for sure is to weigh the known impact of an E&IT solution (i.e. a course) on organizational performance or goals against the cost incurred to create it. Presumably owing to its nature as a unique multinational military defence institution, however, there are limited publications available in the public domain that speak to how NATO builds or revises its training. Accordingly, there is seemingly no publically available research on the potential efficacy or financial cost of any Alliance training. The matter of training efficacy in general is, however, a widely studied topic.

The language throughout NATO's training policy governing the lifecycle of its E&IT initiatives acknowledges the importance of evaluating training efficacy. The structure it uses to guide its training evaluation process is based on the widely accepted Kirkpatrick model, but there appear to be some challenges in how training is constructed and evaluated at the ground level. This article will juxtapose NATO's E&IT policy against relevant research in these fields to identify areas where the Alliance falls short in its efforts to secure a return on its investment in training, and offer suggestions for improvement where possible. Occasionally, arguments will be supported by the empirical observations of the author, who has worked as an E&IT specialist within the NATO cyber community for the last year and a half.

Prior to proceeding, it is prudent to mention that while the experiences referenced within this article occurred during the course of the author's employment with the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), the opinions expressed within are entirely his own and do not necessarily reflect those of the CCDCOE, NATO, or anyone else.

The author would also like to acknowledge that all personnel working to improve the cyber E&IT portfolio of the Alliance are exceptionally hardworking and dedicated professionals. Every success the Alliance has experienced in creating, managing and revising cyber E&IT is due entirely to their ongoing deliberate efforts and commitment. Any problematic issues referenced within this article occurred despite the best efforts of these professionals to prevent them. The challenges identified forthwith are largely systemic in nature and cannot justly be attributed to any negligent or malicious activity.

1 CONTEXTUALIZING CYBERSPACE WITHIN NATO

The first step in the discussion is to contextualize several key pieces of information contributing to the current state of affairs in NATO cyberspace E&IT. In particular, the relative immaturity of the domain and its varying national interpretations have helped to create a situation where the necessary subject matter expertise is somewhat scarce[1].

In a relatively short time, NATO had to figure out how to begin incorporating cyberspace into its existing structures. On the heels of a politically motivated cyber attack on Estonia in 2007, NATO adopted its first cyber defence policy in 2008. In 2014, the Alliance proposed that a cyber attack could possibly lead to the invocation of Article 5, NATO's collective defence policy stipulating that an attack on one Alliance member is an attack on all. Finally, in 2016, NATO recognized cyberspace as a domain of operations (Brent, 2019).

To the layman, this would imply that cyberspace is now placed on an equal footing with its other established domains of operation: air, land, sea and space[2]. One key distinction, however, is that while it is possible to exclusively conduct warfare in cyberspace, the ubiquitous global reliance upon technology makes it almost impossible for any modern military to function independently of cyberspace. NATO recognized this connection in its 2018 »NATO Cyberspace Operations Strategic Training Plan« which, as the name aptly suggests, serves as the Alliance's framework guidance to establishing strategic aims for NATO's E&IT efforts in cyberspace[3].

Developing E&IT solutions that achieve the Alliance's cyberspace needs is anything but straightforward. Larger international entities such as NATO or the EU, for example, were only able to attempt to regulate the domain after individual constituent nations had done so first. As cyberspace is a completely human-constructed domain, how it is defined, used and protected within a nation can greatly vary according to that nation's specific needs. National cybersecurity strategies are uniquely tailored to the needs and priorities of individual nations (ITU, 2021, p 13), meaning nations train and employ people to function within cyberspace in a variety of ways. Conceptual discrepancies in and of cyberspace at the national level impede the Alliance's ability to develop cyber E&IT based upon a common body of knowledge. This is a standard requirement of systematic instructional design (Chyung, 2008, pp 81-87), and indeed a component of the Systems Approach to Training (SAT) model NATO uses to create training (NATO, 2015, para 6-5).

[1] *Many of these particular issues are worthy of research and exploration in their own right; however, their role within this article will be to set the stage for further discussion of other relevant factors.*

[2] *NATO added space as a domain of operations in 2019, after cyber.*

[3] *This document is not available to those working outside of NATO, and hence, it is not cited.*

Foundational discrepancies in and of cyberspace at the national level can alter the speed at which personnel arriving in NATO billets are able to function as needed. The frustration felt by NATO cyberspace personnel over this discrepancy has led to increased demands for the development of common cyberspace domain foundational training. Individual NATO nations have also expressed a desire to build their own cyber E&IT framework in accordance with common NATO standards. Such initiatives are needed, but often difficult to bring to fruition as nations are often reluctant to discuss capabilities and vulnerabilities within cyberspace (Ertan et al., 2021 p 5, 8).

Despite NATO's recognition of how cyber impacts other domains, the Alliance and many of its member nations still struggle with how to best to integrate cyber into joint functions, battle rhythms and existing collective exercises (Ertan et al., 2021, p 7). For example, an existing NATO operational planning course at one Education and Training Facility (ETF) was unable to incorporate many cyberspace planning considerations owing to an already full curriculum and inflexible schedule. To correct this shortfall, an existing CCDCOE course was approved to train operational planners to incorporate unique cyberspace aspects into the established process. However, not all NATO personnel requiring the original planning course need the cyber »top-up« training, suggesting some reluctance outside the cyber community to acknowledge the cyber domain's impact on established norms and practices.

In recent months, the Alliance has made numerous attempts to develop targeted training that will help cyber gain wider acceptance within the Alliance, but there is a current shortage of available NATO expertise to lean on for input. Expertise takes time to develop and is a critical component for developing effective E&IT solutions (Clark, 2008, pp 5-15). Given the limited availability of subject matter experts to support cyber E&IT development, every effort must be made to ensure the best possible use of any contributions they provide.

2 NATO'S TRAINING GOVERNANCE FRAMEWORK – GLOBAL PROGRAMMING

In order to gain a deeper appreciation of the challenges facing the Alliance's cyber E&IT, one must first understand the environment and structures NATO relies upon to effect its E&IT solutions. NATO employs a governance framework called Global Programming to define and satisfy its E&T requirements through the conduct of individual (i.e. courses) and collective (i.e. exercises) training (NATO, 2016, para 2-5 c(2))[4]. Within this framework, NATO places oversight of individual and collective training on Allied Command Transformation (ACT), to meet the operational requirements identified by Allied Command Operations (ACO).

[4] *Technically, the term E&IT (Education and Individual Training) specifically refers to the courses created to meet NATO training, whereas E&T refers to both E&IT (courses) and collective training (exercises) together. Global Programming manages both E&T and E&IT, yet its SAT policy (discussed in Section 5) applies explicitly to the creation and management of E&IT.*

To streamline the process to map its requirements, NATO categorizes its needs into disciplines which NATO defines as »a NATO approved body of knowledge and skills that outlines an existing or evolving E&T requirement« (NATO, 2015, para 2-2). Cyberspace Operations is one such discipline. Both individual and collective training are integral and complementary components of the operational readiness of any discipline[5].

Broadly speaking, Global Programming outlines the roles and responsibilities of all parties in the process to support NATO's E&T requirements. It outlines NATO's responsibility to define requirements (via ACO) and manage the framework itself (via ACT), but it also requires contributions from entities residing outside of NATO's command and control in order to function. Each discipline requires a Department Head (DH) who is accountable to NATO to ensure that training solutions exist to satisfy the evolving requirements of the Alliance (NATO, 2015, para 2-6). To simplify the process, the DH identifies existing courses that meet NATO needs, or leads the process to create new courses as required. The CCDCOE acts as the DH for the Cyberspace Operations discipline[6]. As a NATO-accredited Centre of Excellence (COE), the CCDCOE operates outside NATO's direct influence, but contributes to the development and delivery of NATO training by conducting NATO training and providing subject matter experts and instructors for other ETFs as needed. Finally, ETFs are required to help create and deliver NATO training. All ETF's supporting NATO cyberspace training also operate outside of NATO's direct sphere of influence.

Global Programming is reliant upon specific deliverables and inputs, the quality of which directly correlate to the efficacy of the framework itself. From a business standpoint, it is far more cost effective for NATO to outsource the coordination and creation of these products than to manage them all internally. This planned flexibility allows the Alliance to focus on end results rather than the process by which they are achieved. Unfortunately, the flexibility required to maintain this framework has occasionally forced the Alliance to make certain compromises in its training.

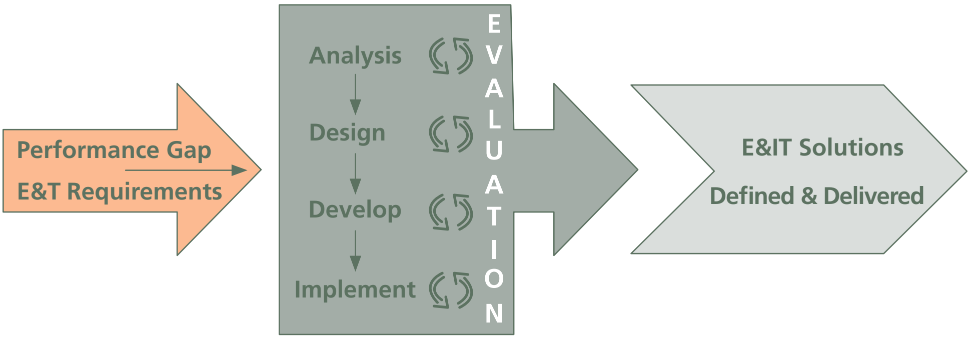
3 NATO SYSTEMS APPROACH TO TRAINING (SAT)

The SAT model that NATO employs within Global Programming to guide the process by which courses are created and maintained (NATO, 2015) is based on the ADDIE model (see Figure 1). This model is a common industry standard systems model for building training, and NATO's own adaptation is based upon a version of ADDIE used by the Canadian Armed Forces to manage its training.

[5] *The primary focus of this article is on individual training with periodic reference to collective training as required.*

[6] *The author primarily works in support of the DH function at the CCDCOE.*

Figure 1: NATO Systems Approach to Training Model (NATO, 2015, para 4-6)



The ADDIE model consists of five phases: analysis, design, development, implementation, and evaluation. These phases are intended to be sequential yet iterative with the success of each phase being largely dependent upon the quality of work produced in the previous phases (Welty, 2008, p 66). The final letter in the acronym, evaluation, has two distinct yet important roles. First, it occurs throughout the process as a measure of periodic quality control. Secondly, it also occurs as a separate and distinct phase after implementation to assess the effectiveness of the solution against the identified problem, and it guides follow-on adjustment activities if required (Chyung 2008, Welty, 2008, p 66). The phases of this model as they pertain to NATO are summarized in Table 1.

Table 1: NATO SAT Overview (prepared by the author)

Phase	Objective	NATO Input	NATO Output	Lead
Analysis	Define the expected performance standards that E&IT will achieve (CCD II)	Determination that E&IT will correct the problem	CCD I (agreement to conduct training) / CCD II (defined performance standard)	DH[7]
Design	Create a structured plan (program) of instruction (CCD III) to train to the standard in the analysis phase	CCD II	CCD III[8] (programme of instruction)	DH / ETF[9]

[7] *Department Head – the entity accountable to NATO to ensure that training solutions exist to satisfy the evolving requirements of the Alliance (NATO, 2015, para 2-6).*

[8] *Course Control Documents (CCD) refer to specific NATO deliverables produced during the NATO SAT process. The core elements captured within CCD II and CCD III reflect requirements of training created via the ADDIE model in settings beyond that of NATO.*

[9] *Education and Training Facility – an institution where NATO training is delivered.*

Development	Develop and/or procure all resources necessary to conduct the course	CCD III	Lesson plans, presentations, training aids, etc.	ETF
Implementation	Deliver the course (ideally first through a »pilot« trial)	Design and development outputs	Trained students	ETF
Evaluation	Assess course integrity to confirm the degree to which the analysis standard was achieved	Trained students	Validated training solution and/or suggested areas of refinement for any/all earlier phases	ETF (internal) NATO (external)

Of note is that prior to engaging any model to develop a training solution (ADDIE or otherwise) a thorough analysis of the performance problem must be conducted to determine the most appropriate means to correct it (Christensen, 2018, p 38). Unfortunately, this critical step is often inadvertently bypassed, thereby immediately placing a proposed E&IT solution on unsteady ground. Premature selection of E&IT creates the illusion that the problem has been solved when perhaps it has not (Shushan, 2012, p 61, Spitzer, 1984, 6). A decision to develop training to correct a performance problem implies an immediate step toward addressing the issue, whereas the necessary step of analysis can sometimes be incorrectly equated with inaction. Even if training is the correct solution for a performance gap, a proper »needs assessment« will provide valuable insight into the nature of the problem, and will help reinforce the quality of the training solution. At the very least, it will ensure that all future work remains aligned with the scope of the original problem (Christensen, 2018, p 38).

Once training is identified as the correct response to address a performance problem, the analysis phase commences. Here, the DH establishes a team of experts and guides them through the process to define clearly the standard of performance that the training solution will eventually achieve. The results of this process are captured within a document NATO calls a CCD II. From a change management perspective, this also helps to define the scope of the deliverables and outlines the desired result that all follow-on work will achieve (James and Ward, 2001, pp 158-159).

During the design phase, the designated ETF creates a programme of instruction outlining the path of learning for the proposed training solution. Within NATO's framework, this document is called a CCD III. On behalf of NATO, the DH is responsible for verifying that the CCD III fully addresses the standard identified within the CCD II. A quality CCD III outlines topics of instruction as well as methods of instruction and assessment. Ideally, the course and its assessments will conceptually emulate working conditions as closely as possible (Coscarelli and Shrock, 2007, p 44). The rationale is that this will stimulate learning transfer, that is, to ensure that the candidate will be able to apply that which they learn during the course within the workplace (Burke and Saks, 2012, p 118).

ETFs within the cyber community proficiently conduct the development and implementation phases within the ADDIE model. These two phases essentially involve preparing and executing the plan as laid out within the CCD III, and lend themselves well to the supervision of a project manager. Most problems, however, reside within the details of the CCD III derived from the design phase. Compromises on the structure and granularity of CCD IIIs can expedite the process by which courses are designed, but it can also affect course integrity[10].

NATO's policy governing the SAT process provides guidance on the requirements of a CCD III. In the author's experience, however, the importance of a CCD III document is often underestimated, due to pressure to quickly move on to subsequent phases where more tangible deliverables are produced. Some ETFs proceed into development once broad training topics are defined. This can lead to gaps or overlaps within a course if the problem is not corrected or losses of time if corrections are ultimately made.

Such a decision can result in flaws within a course that lead it to fall short of intended expectations (Bunch, 2007, p 145). Regrettably, acts of this nature have threatened the efficacy of more than one cyber training solution. Of note, one recent cyber E&IT solution prematurely proceeded to the development phase and had the unintended effect of slowing down lesson plan development. Specifically, subject matter experts were asked to create lessons with only broad guidance on topic and lecture duration, and without addressing the assessment standard that their lessons would ultimately prepare students to achieve. This oversight resulted in increased revision time for some subject matter experts based on back and forth communication with the responsible ETF, and eventually slowed down the process by which the lessons were developed.

Even though the CCD III is the responsibility of the ETF to manage, it is within NATO's best interests to encourage more granularity in the document for newly developed training solutions. Formulating a properly detailed plan before attempting to execute it may give the initial impression that a project is moving slowly, but it will pay off in the long run by limiting the need to revisit and correct previous errors based on goals that were initially unclear or unrefined (James and Ward, 2001). As the old adage suggests, it is best to measure twice and cut once.

[10] *These issues are typically observed during the evaluation process.*

4 CUSTOMER FUNDED EDUCATION AND TRAINING FACILITIES (ETF)

All ETFs that deliver NATO cyber training are customer-funded, which is the norm for the Alliance (NATO, 2015, para 2-12). Under this approach, NATO provides funding to design and develop new courses and to conduct major revisions to existing ones. The ETF itself is responsible for funding the delivery and routine maintenance of its NATO courses. Like any business, customer-funded ETFs must generate more revenue than they expend if they are to operate under this model.

ETFs generally rely upon revenue from tuition to maintain their training portfolios, although some ETFs have additional mechanisms in place to minimize tuition fees. It is also important to note that in addition to design and development costs, NATO is still responsible for paying the tuition of personnel that it sends on training courses. ETFs are also typically free to gain revenue by offering their training to entities outside of the Alliance.

ETFs such as the CCDCOE and the NATO School Oberammergau (NSO) partially subsidize the cost of attending training through established national or governing body funding and the staff provided to them by member nations. Their tuition costs are €500 per course (NATO CCDCOE, 2021, p 12) or €550 per week (NATO School Oberammergau, 2021), respectively. The NATO Communications and Information Agency (NCIA) Academy does not have the same supports at its disposal to subsidize its training and, as such, it relies more on tuition and other fees paid by attendees to cover the operating costs. NCIA training is substantially more expensive at an average cost of €1,100 per week (NCI Agency, 2020, p 17).

Keeping in mind the pressures that all organizations face to manage their budgets, the cost of customer-funded training is of concern to both ETFs that deliver training and any organizations that pay tuition. Some institutions which support the development of cyber training have placed pressure on designated ETFs to reduce tuition in exchange for their services. Such practices have slowed down development on occasion. Other institutions have expressed interest in having new courses developed at ETFs with lower tuition and development costs even if they are less suited to conducting the training in question. Even though the NCIA is the most expensive option for cyber E&IT, it is often easier for them to incorporate new courses into their portfolio than it is for most other ETFs. Opposition to their accepted and transparent business model can, however, contribute to delays in their ability to develop training.

Given the approach of many ETFs to establish tuition costs relative to the duration of their courses, there is often a need for NATO and ETFs to compromise on course content to confine training to one or more calendar weeks. This was the case for the previously mentioned operational planning course, which could not be extended to include additional cyber related content. Spitzer (1984, p 6) cites the practice of allowing such constructs to drive training duration rather than the training requirements themselves as one of 39 reasons why training commonly fails. The fact that most of Spitzer's assertions remain valid nearly 40 years after initial publication speaks volumes about the failure of the education and training community to learn from history.

For one course under development at an ETF, the curriculum identified within the design phase necessitated eight training days; however, the aim was to conclude all training within one week. The increased tuition for an additional week was one factor that contributed to the Alliance's decision to ultimately separate the course into two smaller, sequential ones. In this particular instance, splitting the training was the correct decision. It placed an emphasis on addressing the original identified requirements, and allowed for the development of a desperately needed cyberspace foundational course that is suitable for a much wider audience than the original requirement addressed. This was only feasible, however, because both course projects reside within the same discipline and ETF.

The necessary decision to split this course into two separate ones, however, was not without consequence. The funding provided by NATO to cover design and development costs for the original course was expended. Funding for any additional design and development work for the two new courses could not be obtained. Arguably, any design and development costs for the revised courses would have been minimal, as much of the previously developed resources were still usable, but some work still needed to be done. The absence of funding for this work forced the ETF to find the time and money to make corrections within its existing resources, and was counterintuitive to NATO's SAT process. Specifically, the lack of funding prevented a thorough evaluation of these changes on previous analysis and design assumptions before continuing with development.

5 LACK OF EDUCATION AND TRAINING EXPERTISE

An often overlooked barrier that NATO must contend with in the application of its training model are the assumptions and beliefs held by institutional leadership across all partner entities with regard to E&IT. Most personnel working within the greater NATO training community are unfamiliar with the processes by which courses are created both within NATO, or even in general. There is a widely held misconception that NATO's existing E&IT policy documentation is sufficient in and of itself to help non-experts create and manage efficient training solutions. However, if creating a training solution was as simple and straightforward as reading a book or following a policy, there would likely not be an abundance of research on failed training initiatives.

In practice, individual conflicting interpretations of NATO's E&IT policy documentation, coupled with personal assumptions about training, create more problems than they resolve, and account for the majority of the author's efforts working as an E&IT specialist within the cyber domain. Unfortunately, assumptions made by organizational leadership often prematurely lead to training being identified as the best means to address a performance problem without any noteworthy analysis of the problem itself (Shushan, 2012, pp 61-62, Spitzer, 1984, pp 6-7). As previously suggested, this bypasses the critical first step upon which NATO's SAT model is based – confirming that training is indeed the solution to the identified requirement.

Worse still, many organizations tend to under-support training development initiatives by searching for solutions that are seen as easier or quicker to implement (Spitzer, 1984, p 6), which often results in »counter intuitive behavior« (Betts and Lu, 2011, p 126). Asynchronous online learning solutions that are essentially screen captures of manuals or policies are excellent examples of rushed solutions, yet careful and deliberate planning is an integral component to building successful online training solutions (Ataizi and Durak, 2016, p 2085). While NATO has made significant effort to weed out poorly planned training solutions, one need not look very far to find examples of such courses within the Alliance.

To compound the problem, training is often a »fire and forget« solution. In much the same way that software requires patching to correct newly discovered vulnerabilities, training also requires maintenance driven by deliberate evaluation activities in order to correct unforeseen design errors and remain relevant over time (Betts and Lu, 2011, pp 126-128; Welty, 2008). Once a training solution has been introduced, however, there is a general reluctance by many organizations to commit to performance improvement initiatives (Spitzer, 1984, p 7), despite calls from training experts to do so. This is particularly true in the case of customer-funded ETFs, where dedicating resources to course revision activities may simply be too costly to justify. Common problems of this nature plague the efficacy of training across the globe, and all are present within NATO cyber E&IT.

Often, ETFs rely on project managers to oversee design, development, implementation and evaluation efforts. Their skillset is well suited to shepherding personnel through complex processes; however, if a project manager lacks experience in course development, they can unknowingly take shortcuts during earlier phases that require costly corrections later in the process. Conversely, some E&IT specialists lack the necessary project management background to mitigate the many challenges in balancing organizational demands and the process to create training. Allan Harris' SPADES model addresses ADDIE requirements by leveraging core project management principles that tend to be more familiar to stakeholders (Harris, 2013). Harris' model shows promise as it seeks to optimize the creation of training by sufficiently informing the influential people within an organization who could ultimately be responsible for success or failure. It is worth noting, however, that in order to apply Harris' model, one must also possess a strong working knowledge of the ADDIE model.

Harris' ideas have merit in other research as well. Bunch suggests that training interventions may fail at least in part due to the fact that more dominant cultures within an organization exclude or undervalue the input from less dominant professionals within an organization (Bunch, 2007, p 151), such as E&IT specialists. Similarly, Spitzer suggests that training professionals are partly to blame for training failures by not establishing consulting norms and clarifying management's misconceptions on training (Spitzer, 1984, p 7). This is particularly challenging within multinational military structures, such as NATO, where differing assumptions surrounding rank and expertise can heavily influence the means by which input from a subordinate is heard.

In the Canadian model, upon which NATO's version is based, unit leadership relies heavily upon the input of specially trained military E&IT advisors and instructional designers, called Training Development Officers (TDOs)[11] to shepherd their training processes. At Canadian ETFs, TDOs are most often junior officers (Captain or equivalent) whose expertise resides within the realm of E&IT and not the subject matter trained at their ETFs. The underlying principal is that differing perspectives from content and process experts will provide a more well-rounded solution (Clark, 2008, pp 11-12). While the authority to decide and act within the Canadian military also resides within rank, the culture of senior leadership accepting or at least considering advice from a ranking subordinate expert is the norm. In multinational settings, however, there can be differing perceptions with regard to the connection between rank and expertise. Perceptions of this nature can result in the adoption of ill-informed decisions.

The use of an instructional designer in the process to create education and training is a very common practice, but the value of such expertise is often lost to those who normally work outside of the field of E&IT. Despite working within a national structure that relies upon such expertise, a recent commander of Canada's OPERATION UNIFIER was surprised by how well TDOs contributed to the rotation's efforts to effect meaningful and sustainable change in training the Security Forces of Ukraine. He even posited that Ukraine should seek to develop a similar capacity tailored to their own needs to ensure long-term stability within their training system (Leroux, 2019, p 13).

Within the greater NATO community, there is a dearth of E&IT specialist expertise. The Alliance relies upon the DH and expertise within its ETF to provide similar education and training guidance throughout the SAT process, but this does not always work. The breadth of competing strategic responsibilities placed upon a DH makes it very challenging for them to focus on the tactical details within a particular ETF's CCD III. As previously mentioned, ETFs may not have this skillset on hand, either. Some cyber ETFs have even normalized the practice of having a singular content expert or instructor being responsible for the integrity of a CCD III. If this individual is reluctant to accept advice on the structure of their course from a non-content expert, the effectiveness of the CCD III, and even the integrity of the course itself, may suffer.

[11] *The author is one such Training Development Officer (TDO) within the Canadian Armed Forces (CAF).*

The lack of instructional design experience contributes to the production of curriculum documentation lacking sufficient detail to be of any real use to an ETF. If done properly, the CCD III will not only guide the development process, but it will ensure consistent delivery and management of courses over time. Quite often, these documents are populated only to the depth necessary to demonstrate they meet the NATO requirements contained within the CCD II. Regrettably, this proliferates the impression within ETFs that the CCD III is merely an administrative tool required by NATO.

It is also worth noting that some cyber ETFs do not even require a CCD III or equivalent curriculum document for courses they deliver that reside outside the area of NATO's interest. In these instances, lesson plans and PowerPoint presentations exist in lieu of any structured outline of course content. Courses without controlled curriculum documentation (such as a CCD III or equivalent) are subject to frequent unsupervised revision and can easily evolve outside of their intended scope over time. While not an immediate concern for every ETF, this can present an administrative nightmare to any ETF wishing to demonstrate that one of its existing courses meets a NATO requirement.

6 EVALUATION OF TRAINING

A thorough evaluation of a course will confirm the degree to which it contributes to any recognizable performance improvement, and is the basis for assessing return on investment. If a course can be linked to improving organizational objectives, it is viewed as a success. If the results are less conclusive, revision or removal of the training solution may be warranted (Gagné et al., 2005, p 350). In theory, the evaluative results of a course would be more favourable if the training solution were constructed following the guidance and advice of an instructional designer who followed a SAT model, like the one in use by NATO.

NATO's E&IT policy leverages Donald Kirkpatrick's model of evaluating training across four levels: reaction, learning, behavior and results. This model is a common industry standard for evaluating E&IT efficacy, and is summarized and contextualized for NATO's use in Table 2 (Kirkpatrick Partners, 2022). Most instructional designers leverage the requirements of Levels 3 and 4 while creating course curriculum, and focus on Levels 1 and 2 when developing specific course materials (Gagné et al., 2005, p 351).

Table 2: Kirkpatrick's model contextualized for use in NATO (based on information obtained from Kirkpatrick Partners, 2022, with additional NATO contextualization provided by the author)

Level	What it Evaluates	Achieved by	Responsible Entity
Level 1: Reaction	Student perceptions of training value and quality	Student questionnaires, surveys or interviews during training or shortly after training has concluded	ETF
Level 2: Learning	The degree of student learning attributable to the training	Assessing student performance against the objectives of the training solution	ETF
Level 3: Behavior	The degree to which concepts learned during training are applied on the job	Questionnaires, surveys or discussions with supervisors after training has concluded and former student work performance has had the opportunity to normalize (i.e. 6-12 months after training)	ETF
Level 4: Results	How or whether the training solution has affected organizational needs as intended (return on investment)	Observing performance on missions, operations and/or daily work, or by other quantifiable observable means	NATO

6.1 Level 1 Evaluations

The collection and analysis of Level 1 feedback is a component of the quality assurance model ETFs must conduct while delivering NATO training (NATO, 2015, para 9-5, a). At the moment, Level 1 feedback represents the most prevalent source of concrete and tracked data available to cyber ETFs on the efficacy of their training. As such, this information heavily influences the training maintenance activities that ETF leadership will endorse. If data trends suggest a high degree of student satisfaction, then there is little need for improvement. Relying primarily upon student satisfaction as the main measure of training effectiveness will, however, falsely equate training value with entertainment (Spitzer, 1984, p 8).

Reactionary feedback data is insufficient in and of itself to paint a complete picture of training efficacy (Coscarelli and Shrock, 2007, p 7, Kirkpatrick Partners, 2022). Level 1 feedback is intended to be viewed together with data from all other levels in Kirkpatrick's model as part of a systematic and systemic approach to evaluating a training program's efficacy (Chyung 2008, pp 65-66).

6.2 Level 2 Evaluations

Level 2 data is obtained by assessing student performance to confirm the degree of learning attributable to the training solution (Kirkpatrick Partners, 2022). Formative assessments provide feedback to students to guide their learning process and to identify areas where the ETF can improve learning experiences in the future (Gagné et al., 2005, p 349). Summative assessment confirms student achievement of course objectives, and validates the instructional methods employed by the ETF (Gagné et al., 2005, p 350). NATO's training policy acknowledges both forms of assessment (NATO, 2015, para 7-6) and highlights the importance of summative assessment as the means to confirm that performance gaps have been satisfied (NATO, 2015, para 9-5 b.). The use of summative assessments within face-to-face training, cyber or otherwise, appears to be limited[12]. Asynchronous online courses often contain mandatory summative assessments, yet such tests tend to be constructed and/or administered in ways that do not necessarily confirm the achievement of all the intended learning objectives.

Formative assessments occur reasonably well in most cyber courses, but as they are used at present they do not objectively satisfy the second level of Kirkpatrick's model. The general tendency is to collectively assess student performance in small groups or syndicates. The feedback they receive is normally subjective and based on instructor expertise in relation to the course objectives, rather than a clearly established standard. As most NATO personnel work within a team setting, assessments of this nature at least partially emulate working conditions, which is a core component to successful assessment (Coscarelli and Shrock, 2007, p 44). However, group assessments are not always the best tool to evaluate the content mastery of individual learners. Furthermore, effective assessments need to be constructed against a specified criteria or standard (Gagné et al., 2005, p 350) if they are to consistently and objectively evaluate performance over time (Coscarelli and Shrock, 2007, p 190).

The value of assessment extends well beyond determining whether a candidate »passes« or »fails« a particular course. If training is properly constructed, analyzing student assessment results over time will provide statistical relevance on the efficacy of instruction and learning which can guide any corrective measures of an ETF (Gagné et al., 2005, pp 349-350). A lack of objective summative assessments impedes the Alliance's ability to evaluate a training solution against Level 3 or 4 in Kirkpatrick's model (Coscarelli and Shrock, 2007, p 6). Summative assessment establishes the »chain of evidence« between end of course performance and on the job performance (Gagné et al., 2005, p 348). Without it, there is no way to prove that the training actually improved organizational performance.

[12] *Anecdotally, the rationale for avoiding summative assessments seem to be rooted in concerns over how NATO and its individual nation states might react to unsatisfactory student performance.*

6.3 Level 3 and 4 Evaluations

Levels 3 and 4 of Kirkpatrick's model have the greatest correlation to higher rates of training transfer[13], yet organizations are often hesitant to move beyond Level 2 (Burke and Saks, 2012, p 123). To be fair, however, level 1 and 2 evaluations are much easier for an ETF to effect, as the data comes from their students and is relatively easy to collect. Data of this nature is also easier for an ETF to contextualize and analyze.

Within the training policy documentation, levels 3 and 4 are combined under the label »external evaluations« (NATO, 2015, para 9-5 c). The focus of these evaluations is the job-based performance elements identified within the analysis phase of the NATO SAT process (i.e. the performance standards in the CCD II). Job performance is measured against these standards to confirm the degree to which the objectives of training are truly achieved.

The Alliance relies upon ETFs to conduct Level 3 evaluations, typically via survey or questionnaire. A primary data source for both Level 3 and 4 evaluations is former students and/or their supervisors. Their insight is needed to verify whether the training concepts are being employed in the work place (Level 3) and the degree to which this behavior is benefiting the greater organization (Level 4). The strongest correlation between training transfer and such evaluations tends to be within the period of 6 months to a year after the training has concluded (Burke and Saks, 2012, p 123), a sentiment echoed by NATO's E&IT policy (NATO, 2015, para 9-5). Unfortunately, analysis efforts are often mired by a lack of willingness or ability to participate. Also, if a prospective participant is no longer (or never was) employed in a role where the training is used, their input may not be valid. Given the difficulties of collecting Level 3 data, it is hard to say how the results are communicated between the Alliance and the ETF that delivers the training, but both parties have a vested interest in the conversation.

The degree of accountability respondents have to the Alliance may also impact the training transfer and evaluation process, but the process could be improved if NATO appropriately incentivized participation in Level 3 evaluations (Burke and Saks, 2012, p 125). In order to do this, the work that personnel are doing must be connected to the training they receive and it must be both valued and supported by the organization (i.e. NATO) in order to close the gap between training and the workplace (Spitzer, 1984, p 8; Beer et al., 2016, pp 5-7).

The only way that NATO can address the requirements of Kirkpatrick's Level 4 evaluations is by connecting exercise and workplace performance to the individual training delivered via its ETFs. Exercise and workplace performance are both routinely analyzed by the Alliance, but not necessarily in a manner that provides insight on the training one has received. It is important to note that successful

[13] *Again, transfer of training refers to a student's ability to apply that which they learn during the course within the workplace (Burke and Saks, 2012, p 118).*

performance on an exercise or within the workplace is not necessarily a sufficient indicator of training quality – even for carefully and properly constructed courses.

In order to close the loop on Kirkpatrick's model and calculate any real return on investment for its training, NATO needs to collect and analyze data pertaining to how its training solutions contributed to increased operational performance. This information must be shared with ETFs so that they can adjust their training programs accordingly to ensure Alliance requirements are met.

NATO's training documentation clearly highlights the importance of the information it obtains from external evaluations, but it is deliberately written in such a way as to provide ETFs with flexibility in the manner in which they conduct them (NATO, 2015, para 9-5). Unfortunately, the degree or consistency to which external evaluations are done for cyber training is not widely known.

6.4 Why Evaluation Matters

The aim of any NATO training solution is to correct a noted deficiency that is of concern to the Alliance. A Level 4 evaluation under the Kirkpatrick model seeks to confirm whether the training solution has achieved this aim, but such an evaluation is difficult to undertake and relies heavily upon inputs from Levels 2 and 3 (Coscarelli and Shrock, 2007, p 6). Unless summative assessments are used and Level 3 data collection efforts are prioritized, definitively calculating any true return on investment (via Level 4) will be almost impossible.

In their analysis of why process improvement fails, Betts and Lu (2011, pp 126-128) conclude that in order for training to be successful, it must be developed within a supportive framework that actively imposes an honest continuous improvement process. The framework that they suggest aligns with all the requirements within the ADDIE model, but places particular emphasis on open and honest communication throughout the evaluation process.

As it pertains to NATO, the evaluation phase is disjointed and incomplete. As the driver of requirements, NATO is very influential during the onset of the SAT process, but seemingly less so during the later phases. The Alliance clearly has a vested interest in the success of its E&IT solutions; however, NATO's reliance on external entities outside of its command and control to effect its E&IT efforts has somehow created an environment where the existence of training solutions is valued over their quality.

At the moment, NATO can only attempt to gain feedback on the effectiveness of individual training by assessing performance during its collective training efforts and reviewing what little feedback material ETFs are able to gather. The degree of training transfer will never truly be known unless the Alliance takes deliberate steps to ensure the collection, analysis and socialization of data across all the partners involved in the process.

Conclusion

The previously discussed challenges facing NATO in developing meaningful cyber training vary in severity and risk to the Alliance. To those with only a cursory background in E&IT, many of these risks may not seem overly serious. If left dormant, however, these deficiencies can set the conditions for current and future cyber training initiatives to fall short of expectations and waste valuable and already scarce resources.

Most of the subject matter experts required to create NATO cyber training initiatives work within the operational realm of the Alliance. Accordingly, they are only able to support E&IT projects when operational conditions permit, and when their organizations prioritize their support. Even so, many experts who have contributed to recent cyber E&IT development initiatives have at least partially volunteered their personal time to do so. Given the slow rate at which we are able to develop new solutions based on expertise shortages, it is imperative that NATO optimize its E&IT design and development efforts. Using the Chapman Alliance data to contextualize the gravity of the situation, one hour of instructor-led training can take upwards of 43 hours (approximately $5,934 USD) to create. A one week instructor-led course with 36 hours of instruction would, on average, take roughly 1,500 hours to complete (at a cost just over 200K) (Chapman, 2010). The degree of accuracy behind these figures is less important than the message they convey with regard to the magnitude of effort required to create training.

NATO's training solutions need not be perfect to be effective, but currently their effectiveness is largely unverified and there are some obvious holes in how they are managed. Gaining an appreciation of how these problems may collectively affect the efficacy of current E&IT initiatives will help the Alliance to plan for future success.

If an assessment of a performance problem does not occur, then how do we know training will fix the problem? If the training solution is built upon unsteady ground, or participants have too varied experiences within the subject matter, then how can we plan to build a one-size-fits-all training solution for them? If we restrict course content based on the time available to train and not on the content that is required, how are we providing students with the tools they need to succeed in the workplace? If we do not objectively assess learner performance, how can we ensure learning is occurring? If we do not know whether training is causing changes in personnel behavior and improvements in organizational outputs, then how do we know if the training is even correcting the initial problem? If subject matter expert time is perceived to be squandered, how will we get more support in the future when it is needed?

It is proposed that the Alliance's next cyber training intervention should undergo careful and deliberate planning before fully engaging the NATO SAT model. A dedicated project manager and E&IT specialist should collaborate on this endeavour to ensure the requirements of both the SAT model and organizational stakeholders are sufficiently addressed. The plan should clearly identify the level of support required for all necessary entities at all phases within the NATO SAT model, and prioritize the requirements for deliverables at every step. Once internally approved by the Alliance, the plan will need to be communicated and agreed upon by all stakeholders to ensure project success and enable advanced planning for individual organizational leadership rather than reaction. Only then, should work commence on closing the gap.

At a minimum, this plan should address the following issues:

- Thoroughly assessing a problem before trying to fix it with E&IT;
- A careful analysis of the target audience so as to assess the common starting point and identify potential gap training for some participants as needed;
- A clear emphasis on ensuring quality of SAT deliverables throughout the process;
- Ensuring the necessary content drives training rather than scheduling (minimizing residential training can be offset by leveraging asynchronous online training modules to employ a blended learning approach);
- A requirement to objectively assess student performance (if not to award certification, then to confirm learning at a minimum);
- Identify which entities are required to support the project, and what that support looks like;
- Outline a clear plan to externally evaluate training that is observably endorsed by NATO leadership at the highest appropriate level;
- Ensure that all internal and external evaluation data and analysis is shared between all stakeholders as soon as practicable.

The key to ensuring any change initiative is careful planning and clear and frequent communication. Work of this nature is initially time-consuming, but will ensure higher quality work in the long term. The Alliance need not revise its training policy – yet. Further data is required to assess the existence and magnitude of any perceived holes in their policy before any wide sweeping attempts should be made at correction – this is a clear example of assessing the need before acting.

Piloting and assessing the effectiveness of a slightly revised adaptation to the NATO SAT process would be a more valuable use of time and effort. Specifically, a planned and deliberate attempt to mitigate the known pitfalls coupled with a transparent examination of the results would demonstrate an honest commitment on the part of the Alliance to ensuring training is both efficient and effective. Such a project may uncover more flaws that need to be addressed, or it may even provide a much needed success story.

Bibliography

1. *Ataizi, M., and Durak, G., 2016. The ABC's of online course design according to ADDIE model. Universal Journal of Educational Research, 4(9), pp 2084-2091.*
2. *Beer, M., Finnström, M., Schrader, D., 2016. Why leadership training fails—and what to do about it. Harvard Business Review, October, 2016, pp 50-57.*
3. *Betts, A., and Lu, D., 2011. Why process improvement training fails. Journal of Workplace Learning, 23(2), pp 117-132.*

4. *Brent, L., 2019. NATO's Role in Cyberspace. https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html, 10 February 2022.*
5. *Bunch, K. J., 2007. Training failure as a consequence of organizational culture. Human Resource Development Review, 6(2), pp 142-163.*
6. *Burke, L. A., and Saks, A. M., 2012. An investigation into the relationship between training evaluation and the transfer of training. International Journal of Training and Development, 16(2), pp 118-127.*
7. *Chapman, B., 2010. How long does it take to create learning. http://www.chapmanalliance.com/howlong/ 10 February 2022.*
8. *Christensen, B. D., 2018. From needs assessment to needs analysis. Performance Improvement, 57(7), pp 36-44.*
9. *Chyung, S. Y., 2008. Foundations of Instructional Performance Technology. Amherst: Hrd Press.*
10. *Clark, R. C., 2008. Building Expertise: Cognitive Methods for Training and Performance Improvement. 3rd Ed. San Francisco: Pfeiffer.*
11. *Coscarelli, W. C., and Shrock, S. A., 2007. Criterion-referenced Test Development: Technical and Legal Guidelines for Corporate Training. 3rd Ed. San Francisco: Pfeiffer.*
12. *Ertan, A., Kuprys, A., Lillemets, P., Nordli, G-M., 2021. Cyber Exercises: A Vision for NATO Cycon 2021 Workshop Summary Report. Tallinn: NATO CCDCOE.*
13. *Gagné, R. M., Golas, K. C, Keller, J. M., Wager, W. W., 2005. Principles of Instructional Design. 5th Ed. Belmont, CA: Wadsworth.*
14. *Harris, A., 2013. Training in SPADES. T+D, 67(6), pp 58-62.*
15. *ITU, 2021. Guide to Developing a National Cybersecurity Strategy. 2nd Ed. Geneva: International Telecommunication Union.*
16. *James, M., and Ward, K., 2001. Leading a multinational team of change agents at Glaxo Wellcome (now Glaxo SmithKline). Journal of Change Management, 2(2), pp 148-159.*
17. *Kirkpatrick Partners, 2022. The Kirkpatrick Model. https://kirkpatrickpartners.com/the-kirkpatrick-model/ 10 February 2022.*
18. *Leroux, P., 2019. Security force capability building 2.0: enhancing the structure behind the training. Canadian Military Journal, 19(3), pp 7-14.*
19. *NATO, 2016. Bi-SC Education and Training Directive (E&TD) 075-002.*
20. *NATO, 2015. Bi-SC Education and Training Directive (E&ITD) 075-007.*
21. *NATO CCDCOE, 2021. NATO CCDCOE Training Catalogue, 2022. https://ccdcoe.org/uploads/2022/01/2022_NATO_CCD_COE_Training_Catalogue_FINAL.pdf 15 February 2022.*
22. *NATO School Oberammergau, 2021. Enrolment Instructions. https://www.natoschool.nato.int/Academics/Admin-Info/Enrolment-Instructions, 15 February 2022.*
23. *NCI Agency, 2020. Introducing the NCI Academy. https://www.ncia.nato.int/resources/site1/general/what%20we%20do/nci%20academy/nci_academy_brochure_web_dec20.pdf, 15 February 2022.*
24. *Shushan, E., 2012. Enhance training's worth with learning processes. T+D, 66(2), pp 60-63.*
25. *Spitzer, D. R., 1984. Why training fails. Performance & Instruction Journal, September, 1984, pp 6-10.*
26. *Welty, G., 2008. Formative evaluation in the ADDIE model. Journal of GXP Compliance, 12(4), pp 66-73.*

e-mail: christopher.young@ccdcoe.org

e-mail: christopher.young@ccdcoe.org

Stotnik Christopher Young je magistriral iz upravljanja in pedagoškega vodenja na Univerzi Saint Francis Xavier v Novi Škotski v Kanadi. V kanadskih oboroženih silah se je zaposlil leta 1995. Kot kanadski častnik za razvoj usposabljanja trenutno dela v Natovem centru odličnosti za kibernetsko obrambo (CCDCOE) v Talinu v Estoniji. Deluje v okviru Sektorja za izobraževanje in usposabljanje v CCDCOE kot član vodstvene skupine Oddelka za kibernetske operacije. Podpira vodjo oddelka pri analizi in obravnavi Natovih potreb glede usposabljanj v kibernetskih operacijah.

Captain Christopher Young holds a Masters of Education in Administration and Educational Leadership from Saint Francis Xavier University in Nova Scotia, Canada. He joined the Canadian Armed Forces in 1995. He is a Canadian Training Development Officer (TDO) working at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia. Captain Young works within the Education and Training Branch at the CCDCOE, as a member of the Cyberspace Operations (CO) Department Head (DH) team. He supports the DH in analyzing and addressing NATO's training needs within the Cyber Operations domain.

*Prispevki, objavljeni v Sodobnih vojaških izzivih, niso uradno stališče Slovenske vojske niti organov, iz katerih so avtorji prispevkov.

*Articles, published in the Contemporary Military Challenges do not reflect the official viewpoint of the Slovenian Armed Forces nor the bodies in which the authors of articles are employed.