© ZinetroN/Shutterstock.com

Non-Lethal Measures of Effectiveness in Targeting

By Mr Adam T. Jux, BA, Civilian Targeting Consultant

> *‘Not everything that counts can be counted. Not everything that can be counted counts.’*
>
> William Bruce Cameron

Introduction

In a world of rapid technological advances, specialists in non-lethal warfare face a persistent challenge: measuring the intangible effectiveness of non-lethal operations. Whereas lethal engagements, delivered through land, maritime, and air, often have visible and measurable results, non-lethal effects may have outcomes that are obscured, delayed, or subjective in nature. It is crucial, therefore, to recognize the characteristics and challenges of non-lethal actions by first understanding the current assessment process and then proposing methods which may improve future analysis. Within NATO, there is an ongoing discussion regarding the definition of the terms ‘lethal/non-lethal’ versus ‘kinetic/non-kinetic’. So far, the term ‘lethal/non-lethal’ is used to referring to NATO targeting capabilities.[1] US doctrine, however, uses the term ‘kinetic/non-kinetic’ for capabilities and means, and the term ‘lethal/non-lethal’ for effects.[2] Although there are trade-offs between both framings of the issue, this article will use the NATO lexicon.

Measuring Lethal and Non-Lethal Effects

Military combat performance is typically evaluated through Measures of Performance (MoPs) and Measures of Effectiveness (MoEs):

1. **Measures of Performance (MoP):** Metrics used to determine the accomplishment of actions, answering the question, 'Are the actions being executed as planned?'
2. **Measures of Effectiveness (MoE):** Metrics used to measure a resulting system state, answering the question, 'Did we achieve the intended effects within the planned timescale?'[3]

From a campaign assessment perspective, lethal effects are easier to quantify both in terms of MoPs and MoEs, as they offer tangible metrics, such as the number of tanks destroyed or the percentage of a facility's destruction. However, non-lethal options are often opaque and obfuscated by design. A non-lethal effect often requires extensive time to prepare, execute, and evaluate; incorporating this constraint is particularly important when planning a cohesive Multi-Domain Operation (MDO). Furthermore, it may ultimately contribute to a lethal effect, which complicates MoP and MoE evaluation, as the final target may be degraded or destroyed. Thus, MoPs of non-lethal means may be nearly impossible to assess, whereas MoEs are more likely to be qualitative and may be difficult to attribute directly to the non-lethal effect, but assessment of both will almost certainly be delayed.

Characteristics of Non-Lethal Targeting

Non-lethal targeting can be divided into three focus areas:

1. **Lethal actions with second or third-order non-lethal effects:** This includes exploitation of lethal effects through a non-lethal medium such as strategic messaging following a strike, which requires detailed coordination to ensure complementary and non-detrimental effects.

© ra2 studio/Shutterstock.com

Disinformation – intentionally misleading, false, or biased information – is a potent tool that can persuade numerous influential individuals and the general public by undermining shared understanding and truth.

2. **Pure non-lethal campaigns:** There are many examples of pure non-lethal campaigns. STRATCOM is one such example where there is a need for coordination among all targeting working groups to deconflict and ensure there are no detrimental effects through other campaign methods.
3. **Non-lethal actions complementing lethal actions:** For complex targets like Counter-A2AD, effects planned in all domains should come together and be complementary at the same time to achieve an effect.

Non-lethal targeting includes multiple disciplines with differing procedures and objectives. A selection of these may include:

Strategic Communications (STRATCOM).[4] Strategic communications encompass multiple elements of public diplomacy, political marketing, persuasion, international relations, military strategy, and many other approaches.

These areas can be subdivided into:

1. **Public Affairs (PA).** Engagement through the media to inform the public of policies, operations, military aims and objectives into a timely and accurate manner.
2. **Information Operations (IO).** Creating desired effects on the will, understanding, and capabilities of adversaries and other parties in support of operations, missions and objectives.
3. **Psychological Operations (PSYOPS).** Methods of communications directed at audiences to influence perceptions, attitudes, and behaviour, affecting the achievement of political and military objectives.
4. **Key Leader Engagement (KLE).** Communications and outreach efforts to influential individuals intended to promote awareness of and building understanding and support for policies, operations, and activities.

The assessment of STRATCOM effects can be both quantitative and qualitative, and it is often inferred by examining changing perceptions by way of social media chatter, the tone of media reports, political rhetoric, or trends in public opinion, movement, or preferences. As a cognitive effect, STRATCOM is often divided between strategic long-term objectives and specifically targeted, short-term effects, which can then be fused within the normal targeting cycle. One important characteristic of STRATCOM is that its assessment cannot be judged based on a single report, impression, or observation, but rather, as an evaluation of trends over time. As such, this non-lethal effect is not easily replicated within exercise domains. However, STRATCOM is highly conducive to future Artificial Intelligence (AI)-driven planning, execution, and assessment. Current AI technology already includes regular automated interactions between businesses and consumers, and regularly shapes social media interactions, quantifies audience engagement, and analyses diverse feedback loops,[5] however these commercial applications contrast with military effects due to the availability of measurable metrics.

Civil and Military Cooperation (CIMIC).[6] The military recognizes that not all crises and conflicts require lethal military capabilities, and that crises are often complex and interlinked, requiring whole-of-government subject matter expertise on issues such as ethnic, religious, ideological, and socioeconomic fields. Oversight of these crises therefore requires CIMIC to synchronize management of challenging social, economic, and environmental sectors.

Cooperation and coordination between military forces and local or indigenous authorities is an important and commonly overlooked non-lethal effect, as it may yield more influence than official heads of state at distant capital cities and may enable the achievement of military goals. The importance of shared understanding through cooperative working, liaison, and education needs to be understood so collaborative work, based upon mutual trust and a willingness to cooperate, benefits both sides.

CIMIC provides a crucial non-lethal mechanism for commanders, since the level of human interaction between civil and military personnel facilitates the continual assessment of both the desired interactions (MoPs) and actual results (MoEs). However, this effect must be cultivated continually, and requires extensive and continual investment and foresight to be effective.

Cyber Operations. The cyber domain is relatively new compared to traditional land, maritime and air domains, but it is equally as important and perhaps even more contested, particularly in peacetime. While effects in the cyber domain can be lethal, it is more commonly associated with non-lethal operations. Furthermore, cyber operations are an escalating threat; NATO, which until recently did not have its own cyber capabilities, now faces hundreds of hacking attempts every month.[7] The NATO Cyber Operations Centre (CyOC) in Mons, Belgium recognizes this ever-growing threat from states and non-state actors, hackers, and hacktivists, and can execute operations in response to attacks.[8] There is a perception that cyber acts take place in isolated incidents. However, the Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA), a conglomeration of nations overseen by the CyOC, increasingly understands that cyber incidents represent broad, comprehensive campaigns from both state and non-state actors.[9]

Operational-level JTF commanders own the targeting process and decide which effects to deliver on a given target. However, they will not be able to task any nation to provide such effect. As opposed to conventional means and capabilities, command of national cyber effects will not be ceded to an operational-level commander, as opposed to other conventional capabilities, which upon appropriate transfer of authority will fall under the NATO commander's command and control. Although an effect may be delivered by a nation upon an operational-level commander's request, the nation delivering it will do so on an 'I will tell you what I can do, but not how' basis; here you can see the significance of 'sovereign' in the SCEPVA construct.[10] It is clearly difficult to collaborate when elements are close hold. Notwithstanding long and persistent access to requirements to target networks, many planners can be unaware of available capabilities or what to ask for in order to form a multi-spectral approach to targeting.

The most important thing about NATO's use of cyber capabilities, therefore, is the need to achieve interoperability, starting with an understanding of capabilities to integrate effects into planning cycles. This begins with education in effects and dissemination of SMEs at different levels of command to effectively support and integrate those effects to best fit.

Electronic Warfare (EW). Electronic warfare has been around for well over a century. The first credited use of EW was well documented by Winston Churchill during the Boer War (1899–1902). At the time, the British Army used searchlights to bounce morse code off clouds. This was spotted by The Boers who then tried to jam the signals by using one of their own searchlights in the same fashion.[11]

Today, while EW techniques have evolved considerably, the goal remains largely unchanged – to disrupt or destroy an enemy's ability to observe, orient, decide, and act on the battlefield by degrading, neutralizing, or destroying its combat capabilities. Denial of the electromagnetic spectrum gives a considerable advantage when integrated into a layered, multi-domain attack. Further, the evolution and integration of Cyber Electro Magnetic Activities (CEMA)[12] sees an overlap of two distinct, but complementary disciplines; one primarily concentrated on software and data (cyber), while the other is focused on hardware and signals (EW).[13] Primarily, EW activities are leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system.[14]

It should be remembered that member nations provide specialist support to enhance NATO's capability, which can then lead to problems associated with national security. If member nations provide specialist capabilities, then it is likely that these are sensitive in nature, would not be for public consumption, and would likely need to be kept in a 'grey zone' in terms of deniability and attribution. Thus, nations typically maintain full ownership of those capabilities. This is normal, as opposed to conventional military equipment from member nations that operates under a NATO command structure.

As with other types of non-lethal effects, a dilemma still exists in measuring how well an offensive EW plan has worked. To this end, several MoPs and MoEs are available, including quantifiable parameters such as detecting an adversary's alternative radio frequency, to more subjective parameters, such as the use of electronic

[M] © Marko Aliaksandr/Shutterstock.com

deception to confuse an enemy's Intelligence, Surveillance, and Reconnaissance (ISR) systems. In a recent example, Russia has used the Orlan-10 UAV to insert propaganda SMS messages directly to Ukrainian soldiers by impersonating cell towers and hijacking communications. UAVs, and other platforms, can easily be modified to achieve similar techniques and results, but measuring success will continue to challenge post-targeting assessment due to lagging indicators of effectiveness, such as monitoring defections, changes in patterns of life, and unexpected troop movements in response to propaganda, to name a few examples.[15]

Non-Lethal Considerations

As previously discussed, lethal engagements are often conducive to post-strike analysis, permitting Bomb Hit Analysis (BHA) and Battle Damage Assessment (BDA). However, when targeting cognitive elements, the results can take longer to achieve, and the effects may not always be visible or easily distinguished. Examples of such cognitive elements may be changing a mindset, influencing a population, or forcing a change of posture. General challenges in understanding how to complement effects in those specialist non-lethal fields results in planners not always knowing what effects to ask for and enunciates the difficulty of marrying actions to achieve a synchronized multi-spectrum effect.

All HQs tend to have specialists in non-lethal fields who are integrated into a joint effects branch, but not all specialties are represented at every command echelon. It is imperative, with such long planning times for effects, that all HQs invest in specialist non-lethal fields at all levels of their command structures.

It is reasonable for a Commander to expect feedback regarding non-lethal campaigning, but effects should be expected through broader explanations, as measures cannot be as exact as a number of destroyed tanks following a strike. Have piracy operations stopped within a specific region? Has NATO won support from a host nation through our outreach programmes? Has Nation 'X' stopped supporting and led to more pressure being brought to bear against antagonist Nation 'Y'? These are all reasonable questions for a commander to ask regarding non-lethal campaign development.

It is expected that many answers would be drawn from trends over time, but favourable situations can be exploited in real-time for further gains, and this is the fusion of effects within an MDO construct. A host nation's piracy problem may be influenced through aggressive patrolling, strategic messaging regarding presence of deterring vessels, or cooperation to train and embolden that host nation to be self-sufficient in the future, as well as media campaigns showing NATO as a force for good and the good work of the nation in question. A full-spectrum approach to a problem, but one that can be exploited by a strike against a piracy stronghold with follow-on messaging.

'Measuring Effectiveness in the Information Environment' highlighted where planners of non-lethal actions should have an expectation of second or third order effects before achieving goals.[16] Each effect results in corresponding reactions in a complex, tiered set of causes and effects that need to be interpreted so as to assess the overall impact. An example of this would be effects resulting from an attack against enemy information systems (first order), setting out to achieve an effect on information and information flow (second order), to seek to achieve an impact on an enemy Commander's decision-making (third order and the intended target), requiring an inductive analysis of intelligence reporting and assessments.

However, not every situation requires an MDO solution, but better education and understanding of multi-domain effects will improve the utilization of non-lethal actions and result in a vast array of potential options to Commanders. As member states embrace the MDO concept, the Alliance's integration at the strategic and operational levels should significantly improve regarding targeting as old and varied Tactics, Techniques and Procedures (TTPs) are replaced.

M Jets/Background: © Mike Mareen/Shutterstock.com; Network Pattern: © Irvin 2809 – stock.adobe.com

Multi-Domain Considerations

While the term has been around for a several years, MDO is a NATO operations concept where synchronization and collaboration between the military domains and the other Instruments of Power (IoP) create effects in the physical, cognitive and virtual dimensions. Whereas the term Joint is commonly used within current command structures to describe inter-service deconfliction and teamwork, MDO promotes service-agnostic, domain-oriented coordination, including both military and non-military stakeholders, which is the key differentiation between the two terms.[17] The varied complexities of non-lethal assessment are enunciated further through not only coordination with other domains, but finding a cohesion of effects amongst non-military stakeholders, including political domains, economic domains, Non-Governmental Organizations (NGOs), etc. The list is not exhaustive, but whilst it might seem easy to control the flow of information within a military context, the same cannot be said within non-military organizations and decision timelines.

Examples of non-military non-lethal targeting might include sanctions, seizure of assets, etc. Clearly, from a military perspective, NATO would not wish to undermine a member nation's government by having a lethal effect against assets that would otherwise be seized in order to bring pressure against the owner and maintain a non-escalatory posture. How should those two actions be deconflicted or synchronized?

Recommendations

Having considered the challenges and considerations pertaining to the evaluation of non-lethal effects, we propose three overall recommendations:

1. **Review Non-Lethal Targeting Education.** Education is key for integration and understanding of non-lethal effects. Current NATO targeting training does not cover all specialist non-lethal fields and national assessments have documented this as an area that is lacking.[18] It is common for planners and leadership to underutilize or undervalue speciality fields due to a lack of familiarity, especially in terms of their time requirements and risk analysis.
2. **Adopt MDO as concept and doctrine.** MDO are not required for every target but will improve understanding across the force. Establishing a liaison element or representation at the strategic level in order to deconflict non-military targeting and complement non-NATO actions should be considered and be understandable to planners within the NATO command structure through doctrine.
3. **Invest in computer-aided analysis tools.** Training within the cognitive space should consider the benefits of including AI-generated models to assist with assessment and MoE.

© lavitrei/Shutterstock.com

Conclusion

Advances in battlefield C2, the proliferation of advanced unmanned systems, and the proliferation of EW capabilities among state and non-state actors, makes it critical that commanders understand and maximize their own non-lethal capabilities. While non-lethal targeting is difficult to quantify, commanders have several tools available to maximize the planning, execution, and evaluation of non-lethal effects in the battlespace. First, they must educate themselves and their service members concerning the capabilities and limitations of non-lethal effects. Second, they must demand deeper and more thorough integration across domains and services. Finally, they must promote and utilize emerging technologies which promise to reduce planning, execution, and analysis timelines. By understanding the importance of non-lethal effects, managing expectations, and pursuing new processes and tools, they will expand their warfighting tool chest for tomorrow's conflict. ●

1. https://assets.publishing.service.gov.uk/media/618e7da28fa8f5037ffaa03f/AJP-3.9_EDB_V1_E.pdf
2. https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-60/3-60-Summary-of-Key-Changes.pdf
3. Definitions – CIMIC Handbook (cimic-coe.org).
4. StratCom | NATO Strategic Communications Centre of Excellence Riga, Latvia (stratcomcoe.org).
5. https://www.researchgate.net/publication/379299506
6. NATO and a comprehensive approach – CIMIC Handbook (cimic-coe.org).
7. NATO cyber command to be fully operational in 2023 | Reuters.
8. Ibid, 5.
9. Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) – Cyber Defense Magazine.
10. Ibid, 7.
11. Churchill, W. S. (1900) London to Ladysmith via Pretoria. London. Longmans, Green, and Co.
12. Cyber Electro Magnetic Activities (CEMA) – EMSOPEDIA.
13. Blurring the Lines: The Overlap Between Cyber and Electronic Warfare (jedonline.com).
14. https://securityanddefence.pl/pdf-103299-36215?filename=Electronic%20warfare%20in.pdf
15. SAIC | Why Integrated Electronic-Cyber Warfare Is Crucial.
16. https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/3F_Measures_of_Effectivenes_In_the_Information_Environment.pdf
17. Multi-Domain Operations in NATO – Explained – NATO's ACT.
18. Integrating Lethal and Nonlethal Effects > Air Land Sea Space Application (ALSSA) Center > News (alsa.mil).

ABOUT THE AUTHOR

Mr Adam T. Jux

Civilian Targeting Consultant

Mr Adam T. Jux is a retired Royal Air Force Officer who served in the Royal Australian Air Force and the Australian Army over his 27 years of military experience. He is a qualified targeteer and has worked in the discipline for the last 14 years, including on operations. He has instructed in targeting and collateral damage estimation and has mentored targeting at the Joint and Component levels. He has published a number of articles and contributed to white paper research regarding targeting in general and its interaction with intelligence and other disciplines, and is an advocate for targeting development and doctrine. He is currently working as a civilian targeting consultant for NATO's Joint Warfare Centre in Stavanger, Norway, under contract for Calian Europe AS.