Energy Security in the Era of Hybrid Warfare

(STO-TR-SAS-163)

Executive Summary

NATO's military logistics and supply chain systems are now challenged by the tyranny of distance, near peer adversaries, and tight energy in a manner unseen since World War II. Furthermore, the Operational Energy (OE) requirements of the Alliance's war fighters continue to increase sharply due to the greater energy intensity of sophisticated platforms necessary to enhance force mobility, lethality and operational tempo. Compounding this demand for energy is a lack of investment and poorly conceived and executed plans at decarbonization, which have created national security vulnerabilities. These challenges are exacerbated by new strategies, operational constructs, force designs, and new and emerging weapons / platforms that increase the complexity and dynamics of OE management. Closely related, planners do not appreciate the tactical and operational impact of energy, which could limit capabilities, notably in projecting kinetic effects beyond a single mission, particularly in a contested environment. Ultimately, the inability of the Alliance to better integrate OE management could imperil its forces and mission success.

The ability to leverage technology for geo-political gain against an adversary's vulnerabilities, broadly referred to as hybrid warfare, has become increasingly prevalent in the 21st Century. Hybrid warfare has multiple synonyms, such as "grey zone warfare / strategies," "competition short of conflict," "active measures," and "new generation warfare." Despite differences in terminology, these definitions point to the same fundamentals; in its most basic context, hybrid warfare's genesis can be traced to the age-old principle of asymmetrically exploiting an adversary's weaknesses, with clear 21st Century attributes. This is done by using or 'misusing' capabilities meant to serve the public at-large – either through the commodities it consumes or the public goods and services by which everyone carries out their daily affairs.

The project's focus on energy security is rooted in the pretext that it is fundamentally the most vulnerable sector and possesses the largest potential to destabilize a society. Yet, what does this mean in a practical sense? How can NATO and the member states develop actionable policies and countermeasures? Moreover, from an energy security perspective, this study's primary focus, how can we protect the infrastructure and recover from attacks against this most vital of sectors? Although sovereign nations maintain responsibility for the integrity and defence of their energy infrastructure, NATO operations will require a unified response and a resilient international energy supply coordinated with alliance, European Union, and national objectives.

It is acknowledged that NATO has a role at the forefront of the confluence of energy security, cyber security and hybrid warfare. Within the context of NATO energy security, hybrid threats can be identified as actions by state or non-state actors aimed to undermine or harm NATO's assured access to affordable and acceptable supplies of energy and the ability to protect and deliver sufficient energy to meet mission essential requirements by influencing its decision-making at the local, regional, state, or institutional level.

Additionally, we need to keep in mind the two main components of the hybrid warfare and energy security dynamic are cyber defence and malign influence. NATO has maintained a constant though evolving role in addressing cyber as a hybrid threat to the Critical Energy Infrastructure (CEI) of its member states. Over the past two decades, cyber-attacks against Industrial Control Systems (ICS) of NATO member states' energy supply chains have grown exponentially.

The primary objectives of SAS-163 have been to:

1) Raise awareness of the energy-hybrid warfare nexus;
2) Identify its broader impact in the civilian and military realms within NATO; and
3) Define courses of action.

This includes mitigating the impact on civilian and military infrastructure and interests and develop countermeasures. Ultimately, the project's goal has been to provide analytic support to NATO's civilian and military leadership.

The key findings from the study can be categorized as follows:

- Near-term energy insecurity among the NATO Member States.
- Persistent cyber threats to the energy sector.
- Energy sector supply chain vulnerabilities.
- Impact on NATO's operational energy and military capabilities.
- Malign influence in the energy sector can have significant consequences.

The study recommends continued analysis in the topic of hybrid warfare and energy security, particularly with a focus on NATO eastern tier, arguably the most vulnerable sector, and a deeper investigation of cyber advance warning technologies. For this reason, we have submitted a proposal for a three-year study extension.

La sécurité énergétique à l'ère de la guerre hybride

(STO-TR-SAS-163)

Synthèse

Les systèmes logistiques et chaînes d'approvisionnement militaires de l'OTAN sont désormais confrontés à la tyrannie de la distance, à des adversaires aux capacités presque comparables et à une raréfaction de l'énergie, et ce, d'une manière inédite depuis la seconde guerre mondiale. De plus, les besoins en matière d'énergie opérationnelle (OE) des combattants de l'Alliance continuent d'augmenter fortement à cause de l'intensité énergétique accrue des plates-formes sophistiquées qui améliorent la mobilité des forces, la létalité et le rythme opérationnel. Cette demande d'énergie s'accompagne d'un manque d'investissement et de plans de décarbonation mal conçus et mal exécutés, ce qui a créé des vulnérabilités sur le plan de la sécurité nationale des pays. Ces problèmes sont exacerbés par de nouvelles stratégies, de nouveaux concepts opérationnels et de nouvelles conceptions des forces, ainsi que par des armes/plates-formes nouvelles ou émergentes qui accentuent la complexité et la dynamique de gestion de l'OE. Autre aspect étroitement lié, les planificateurs n'apprécient pas les implications tactiques et opérationnelles de l'énergie, susceptibles de limiter les capacités, notamment lors de la projection d'effets cinétiques au-delà d'une seule mission, en particulier dans un environnement contesté. Enfin, l'incapacité de l'Alliance à mieux intégrer la gestion de l'OE pourrait mettre en péril ses forces et compromettre la réussite de ses missions.

L'exploitation de la technologie pour tirer un avantage géopolitique des vulnérabilités d'un adversaire, généralement désignée par l'expression « guerre hybride », est de plus en plus fréquente au 21e siècle. La guerre hybride a plusieurs synonymes, tels que « guerre/stratégies de zone grise », « concurrence sans conflit », « mesures actives » et « guerre de nouvelle génération ». La terminologie diffère, mais s'appuie sur les mêmes fondements ; à la base, la guerre hybride découle d'un principe vieux comme le monde (exploiter de manière asymétrique les faiblesses d'un adversaire), et y applique les caractéristiques du 21e siècle. Elle consiste à utiliser ou « détourner » les capacités destinées à servir le grand public, soit par le biais des marchandises qu'il consomme, soit par le biais des biens et services publics grâce auxquels chacun mène ses affaires quotidiennes.

Le projet se focalise sur la sécurité énergétique parce qu'il s'agit au fond du secteur le plus vulnérable, qui présente le plus grand potentiel de déstabilisation d'une société. Cependant, qu'est-ce que cela signifie concrètement ? Comment l'OTAN et les États membres peuvent-ils élaborer des politiques et contre-mesures applicables ? En outre, du point de vue de la sécurité énergétique, objectif principal de la présente étude, comment protéger l'infrastructure et rétablir le fonctionnement après d'éventuelles attaques contre ce secteur vital ? Bien que les pays souverains conservent la responsabilité de l'intégrité et de la défense de leur infrastructure énergétique, les opérations de l'OTAN nécessiteront une réponse unifiée et un approvisionnement énergétique international résilient, coordonné avec l'alliance, l'Union européenne et les objectifs nationaux.

Il est reconnu que l'OTAN joue un rôle d'avant-garde à la confluence de la sécurité énergétique, de la cybersécurité et de la guerre hybride. Dans le contexte de la sécurité énergétique de l'OTAN, les menaces hybrides peuvent être définies comme des actions menées par des acteurs étatiques ou non étatiques afin de saper ou compromettre 1) l'accès assuré de l'OTAN à des approvisionnements énergétiques abordables et admissibles et 2) la capacité de protéger et fournir suffisamment d'énergie pour répondre aux besoins essentiels de la mission, en influençant son processus décisionnel au niveau local, régional, étatique ou institutionnel.

Nous devons également garder à l'esprit que les deux principales composantes de la guerre hybride et de la dynamique de sécurité énergétique sont la cyberdéfense et l'influence malveillante. Bien que son rôle ait évolué, l'OTAN a toujours traité la dimension cybernétique comme une menace hybride pour les infrastructures énergétiques critiques (CEI) de ses États membres. Ces deux dernières décennies, nous avons constaté une multiplication des cyberattaques contre les systèmes de contrôle industriel (ICS) des chaînes d'approvisionnement énergétique des États membres de l'OTAN.

Les principaux objectifs du SAS-163 étaient de :

1) sensibiliser aux divers aspects de la guerre hybride énergétique ;
2) identifier son impact au sens large dans les domaines civil et militaire au sein de l'OTAN ; et
3) définir des modes d'action.

Cela inclut le fait d'atténuer l'impact sur les infrastructures et intérêts civils et militaires et d'élaborer des contre-mesures. Pour finir, le but du projet était d'apporter un soutien analytique aux dirigeants civils et militaires de l'OTAN.

Les conclusions essentielles de l'étude peuvent être résumées ainsi :

- Insécurité énergétique à court terme parmi les États membres de l'OTAN.
- Cybermenaces persistantes pour le secteur de l'énergie.
- Vulnérabilités de la chaîne d'approvisionnement du secteur énergétique.
- Impact sur l'énergie opérationnelle et les capacités militaires de l'OTAN.
- Une influence malveillante dans le secteur de l'énergie peut avoir des conséquences importantes.

L'étude recommande une analyse continue de la guerre hybride et de la sécurité énergétique, en particulier dans la sphère occidentale de l'OTAN, sans doute la plus vulnérable, et une enquête plus approfondie sur les technologies cybernétiques d'alerte préalable. C'est pourquoi nous avons soumis une proposition pour prolonger l'étude de trois ans.