Integrating and Shaping Military Cyber Defence in Operational and Intelligence Planning

Joseph JONES
Founder, OS2INT, Skive, Denmark
joseph.jones@os2int.com

Abstract

The cyber threat landscape has undoubtedly evolved at an exponential rate. As such, NATO and EU forces have transformed their capabilities to meet present-day operational challenges in cyberspace. However, this paper will not only identify relative successes by NATO and EU forces with regards to their respective development of cyber defence capabilities, it will also indicate limitations with regards to the projection of power within cyberspace and the lack of national and international coordination concerning offensive cyber operations and the collection of intelligence from cyberspace.

Index terms: cyber capacity building, cyber defence, cyber intelligence, military cyber operation

1. Introduction

This chapter will discuss how the present-day cyber threat landscape has significantly evolved to an extent where cyberspace is now considered a fourth operational arena for military forces. By analysing how competing militaries have transformed their capabilities and exercised unrestrained information maneuver in cyberspace, this article will point out inadequacies within NATO and the EU's unified approach towards hostile cyber threats, namely because of a lack of coordination and interoperability with regards to Offensive Cyber Operations and intelligence-gathering. In conclusion, this article will point out that competing military forces continue to re-shape and refine their mode of operations within cyberspace, NATO and EU military forces will remain restricted in their capability to disrupt hostile cyber threats and deny such threats with the ability to maneuver within cyberspace. Furthermore, the article will recommend greater interoperability between NATO and EU members across all operational spectrums including Offensive Cyber Operations and intelligence-gathering.

2. The Future-Force Concept of Operations in Cyberspace

Not only do state-aligned cyber threats continue to evolve, yet increase in terms of their overall lethality, hostile militaries are widely known to have taken effective steps to integrate military offensive and defensive capabilities across the entire spectrum of military and intelligence capabilities, from tactical-level military formations to strategic-level military intelligence agencies. In light of the rapidly evolving threat, western militaries have a clear requirement to adapt to this rapidly evolving threat by transforming their own military structures and implementing required cyber capabilities.

The UK Ministry of Defence [1] defines cyber operations as the "planning and synchronizations of activities in, and through, cyberspace to enable freedom of maneuver and to achieve military objectives". When clearly defining the categories - or roles - of cyber operations, the following is deemed to be a more concise range of terminology:

- **Offensive Cyber Operations:** Activities that are designed to project power and to enable militaries to achieve their tactical, operational, and strategic objectives in cyberspace.
- **Defensive Cyber Operations:** Activities that include the conduct of active and passive measures aimed at preserving the military's use of cyberspace and enable information maneuver.
- **Cyber Intelligence, Surveillance and Reconnaissance:** A broad array of intelligence, surveillance, and reconnaissance (ISR) activities conducted across the entire spectrum of cyberspace including friendly, neutral and enemy domains in order to strengthen understanding and complement existing ISR activities.

For its part, the North Atlantic Treaty Organization (NATO) and the European Defence Agency (EDA) have developed and implemented their own cyber defense architecture frameworks to address the highly militarized cyber threat landscape whilst offering member states a common approach that promotes inter-operability. That said, the onus remains on individual members to shape their capabilities and build effective capacity within military formations in accordance with the strategic aims of NATO and the EDA. In their respective Architecture Frameworks NATO [2] and EDA [3] only addresses cyber defense operations, ultimately achieving some level of interoperability between NATO and / or EDA member countries with regards to Defensive Cyber Operations and to a lesser extent, Cyber Intelligence, Surveillance and Reconnaissance. However, there remains an overall lack of interoperability and a common approach with regards to Offensive Cyber Operations across NATO and EU member states.

The integration of military cyber capabilities should only take place within the scope of a wider transformation that addresses current and emerging threats. The best-case study from which to explain how NATO and EU member countries should build operation cyber capacity would be to look closely at the UK's 'Future Force Concept'. Describing this concept, the UK Ministry of Defence [4] indicates that the concept is best described as an over-arching programme that encompasses a series of transformation projects ranging from the implementation of advanced soldier systems (clothing, personal weapons and protective solutions) to the reorganizing of military units in accordance with the UK's National Security Capability Review 2017 [5] and its successive Integrated Review of Security, Defence, Development and Foreign Policy 2021 [6]. The latter of which concluded the need for the UK to develop a new National Cyber Force and Counter-Terrorism Operations Centre which covers the full extent of internal and external security threats. As such, the Future Force Concept sees that the future British military will become a threat-integrated, but comparably small fighting force. Additionally, the Future Force Concept also recognizes that technology will remain a significant factor in any future conflict and a significant factor that drives change in the military.

Whilst it is recognized that any threat review or analysis undertaken by NATO and / or EU member countries is likely to be conducted in isolation - as a direct result of classification restrictions and the use of intelligence sources whose details need to be adequately protected - open-source information should be considered.

3. The Role of Cyber Capacity Building

Cyber capacity building encompasses the development and implementation of cyber capabilities through the integration of technology, provision of training and mentoring, and the wider implementation of national-level reform. It should also be strongly based on the outcomes of an integrated threat review / analysis and be driven by Defence and industry partners cross-government within two clearly defined parameters: Force Development and Force Generation.

Force Development within the scope of cyber operations of a cyber military force should be a joint force effort that encompasses the full spectrum of military functional areas including Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance - otherwise referred to as 'C4ISR'. When developing and enacting Force Development, it should follow the following key processes:

- **Force Design:** The desired scope and structure of the cyber force should address the key outcomes of the Threat Review and keep within the parameters outlined within the military's wider operational commitments. Specifically, it should take into account the availability of personnel, funding and systems.
- **Structural Development:** Like the wider military, the cyber force should have a clear structural leadership that is clearly designed and implemented according to the C4ISR functional areas concept.
- **Talent Acquisition:** The bulk effort within the Force Development phase, talent acquisition should be a joint effort from across the military to identify and acquire the necessary talent for cyber operators from the enlisted ranks. It can be argued that the role of cyber operators should be filled from personnel from J2 (Intelligence) and J6 (Communications) functional areas; this is based primarily on the fact that cyber operations require a higher level of technical expertise and certainly requires an intelligence-driven approach. Going further, the identification and acquisition of talent should also be driven by a corporate-level initiative that aims to recruit part-time specialists - or cyber reservists - within the cyber and EMA industry that will also make way for high-level training and mentoring to naturally evolve. Again, it can be argued that the process of talent acquisition for cyber operations specialists should be conducted across J2 and J6 functions to ensure that technical expertise and intelligence capabilities are fully satisfied in this regard.

Force Generation is best described as the physical processes employed by the military to implement capabilities within its cyber force. By default, it is a circular process that constantly evolves, and is designed to take place in concert with Force Development. The generation of the cyber force should be driven by the overall needs of the armed forces as opposed to the needs of individual services. Concurrently, it should also be reinforced by a corporate-level programme from which specialist-level training and capabilities are implemented. Force Generation can be further described by the following processes which should occur in the following order, though overlaps may take place:

- **Education**: A comprehensive education curriculum should be devised and implemented across any new or existing cyber force. It should be focused on indicating how Cyber and EMA activities intend to integrate into the wider military and in what operational spectrums it intends to support, and how. This education should be continuously devised and implemented across the force as opposed to being delivered irregularly.

- **Force Management**: With the structure of the cyber force constructed and required talent acquired, a management structure should be devised and implemented consisting of generalists and specialists with clear roles and responsibilities.
- **Systems Integration**: In accordance with the Threat Review and wider Defence Review, the necessary systems required for any new or existing cyber force should be acquired and integrated as per the military's budget allocation and procurement rules. Systems include general and specialized hardware, hardware and software, and access to third-party intelligence.
- **Specialized Training**: The design, development and implementation of specialized training should take into account individual roles within the cyber force in addition to the range of systems that cyber operators will be expected to use. For the most part, such training will naturally be provided by systems providers; remaining training themes including intelligence collection techniques, penetration testing and malware analysis (to name but a few) should be designed and delivered by competent third-party service providers. Specialist training should also be balanced against the cyber force's current needs and the needs identified during the Force Development stage.
- **Red and Blue Team Exercises**: Activities in the form of exercises should be designed and delivered over regular periods in order to maintain the overall readiness of the cyber force and to ensure that capability gaps are effectively identified and addressed. Additionally, the wider military should adapt existing military exercises to include cyber-related serials for example, cyber and electro-magnetic attacks targeting Battlegroup, Brigade and Divisional-level formations. Lastly, the cyber force should also play an integral part in multi-national NATO and EU Battlegroup (EUBG) exercises.

4. Strategic-Level Capability Development

In its 2018 Framework for Future Alliance Operations report, NATO detailed the future scope of joint operations, indicating that operations in cyberspace would not only see a significant increase but would grow to become more inter-twined with joint ground, air and sea operations [5]. Meanwhile, the UK's Future Force Concept envisages that the British Armed Forces will become increasingly involved in joint NATO-EU operations as opposed to engaging in unilateral conflicts [4]. As such, both of the aforementioned reports emphasize a greater effort towards developing inter-operable capabilities, cross-domain effects, systems and doctrine.

Each NATO and EU member country will inevitably structure their strategic-level cyber capability differently than others - most likely due to their own interpretation of threats and military requirements. Until the mid-2000s, most of the larger NATO member countries including the United States, United Kingdom, France and Germany structured their strategic-level cyber capability along the lines of their own communications intelligence agencies, sometimes augmented by military intelligence specialists. In the United Kingdom, strategic level cyber was almost exclusively led by the Government Communications Headquarters (GCHQ), working alongside strategic partners namely their 'Five Eyes' partners in the United States, Canada, Australia and New Zealand. However, following the National Security Strategy and Strategic Defence and Security Review 2010, the United Kingdom saw strategic-level cyber operations delegated to a centralized joint military and intelligence capability responsible for overseeing national-level cyber operations and the delegation

of capabilities to operational and tactical formations - primarily within Force Troops Command, also known as the 6th (United Kingdom) Division [7].

5. Conclusion

An increase in Russian and Chinese information maneuver within cyberspace has inevitably focused the attention of NATO and EU members to increase their capacity to counter this evolving threat. Whilst noticeable efforts to increase the cyber defense posture of Western countries and enhance interoperability between them is evident, a considerable lack of interoperability with regards to offensive cyber operations and cyber intelligence-gathering has been observed. Additionally, there remains a lack of a unified approach by NATO and EU member states with regards to the design and implementation of inter-operable cyber capacity building programmes. In stark contrast, both Russia and China have taken into consideration the evolving nature of the modern battlefield by shaping their military approach to operations in cyber space. Individually, several NATO and EU member states have unilaterally begun re-shaping their military capabilities, though such transformation programmes - such as the United Kingdom's 'Future Force Concept' - does not address the need for processes and systems to be interoperable with NATO and EU allies.

Moving forward, the raising of capacity and the development of cyber capabilities within strategic-level formations should undoubtedly be driven by the need to increase interoperability and joint operations between NATO and EU member countries. As such, the development of doctrine, implementation of red and blue team exercises in addition to exchange programmes should actively be encouraged. Whilst interoperability with regards to Cyber Defence Operations is somewhat reinforced within the NATO Architectural Framework [3] and the EDA's Cyber Defence Refence Architecture [2]; the lack of interoperability with regards to Offensive Cyber Operations and Cyber Intelligence, Surveillance and Reconnaissance reinforces the requirement for greater-level cooperation between countries and their respective militaries. Indeed, it is likely that NATO and the EDA view Offensive Cyber Operations and Cyber Intelligence, Surveillance and Reconnaissance to be the sole responsibility of its individual members, though it can be argued that the current cyber threat environment reinforces the need for greater interoperability in this regard.

References

[1]. 2018. Future Force Concept (Joint Concept Note 1/17). [ebook] Ministry of Defence. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643061/concepts_uk_future_force_concept_jcn_1_17.pdf [Accessed 3 April 2022].

[2]. "Cyber resilience, a prerequisite for autonomous systems - and vice versa," Default. [Online]. Available: https://eda.europa.eu/webzine/issue16/cover-story/cyber-resilience-a-prerequisite-for-autonomous-systems-and-vice-versa/. [Accessed: 04-Apr-2022].

[3]. North Atlantic Treaty Organization, "NATO Architecture Framework (Version 4)," North Atlantic Treaty Organization, 2020. https://www.nato.int/nato_static_fl2014/assets/pdf/2021/1/pdf/NAFv4_2020.09.pdf (accessed Apr. 04, 2022).

[4]. "Development, Concepts and Doctrine Centre Future Force Concept." [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643061/concepts_uk_future_force_concept_jcn_1_17.pdf.

[5]. North Atlantic Treaty Organization, "Framework for Future Alliance Operations, 2018 Report" North Atlantic Treaty Organization, 2018. https://www.act.nato.int/images/stories/media/doclibrary/180514_ffao18.pdf.

[6]. "Global Britain in a competitive age. The Integrated Review of Security, Defence, Development and Foreign Policy." [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf.

[7]. "National Security Capability Review." [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf.