Avoiding Cyber Forever Wars

IV

Toward a Joint All Domain Whole of NATO Cyber Conflict Deterrence Strategy

By Ms Gentry Lane
ANOVA Intelligence

Cyberspace is poised to be the next 'forever war' battleground unless US and NATO allies change course from the current balkanized, defence-prioritized posture and enact a unilateral deterrence strategy. Cyberspace as an operational domain is rife with peculiarities that create an advantageous battlespace for adversaries. The lack of traditional visibility, ease, and efficacy in executing Offensive Cyber Operations (OCO) are favourable, especially for adversaries who prioritize stealth, persistent degradation of allied institutions in their national interest objective and wish to achieve these objectives without triggering traditional armed conflict. To disallow further adversary advancement in the Cyberspace domain, it is imperative that NATO partners accelerate agreement on desired ends, cohesive strategies, and a quantifiable framework for assessing the progress of ways and means established to deter adversary cyber aggression. The cost of inaction is too great to disregard or delay.

Cyber Conflict

For the purpose of clarity, 'cyber conflict' means aggression between Westphalian nation-state military forces with cyber combatant commands.[1] Cyber conflict can be split into two categories: peacetime aggression and wartime conflicts. (And for the purpose of this paper, 'peacetime' means any period of time outside of congressionally declared war). Unlike warfare in traditional domains, the inevitable wartime cyber conflict will not manifest as the culmination of escalating peacetime cyber aggression. Wartime cyber conflict objectives and targets will be quite different, despite indistinguishable cyber techniques, tactics, and procedures. Military Command and Control (C2) systems, transportation systems, logistics supply chains, and defence suppliers will be the high-value targets during wartime which are accessible via the Cyberspace domain. Whereas during peacetime, strategic military and intelligence assets still rank as high-value targets, but adversaries focus cyber aggression on civilian sector critical infrastructure (private-sector financial institutions, technology providers, telecom, power and water utilities, healthcare systems, etc.) and prioritize self-enrichment via industrial espionage over pure military objectives.

These peacetime and wartime military operations in the Cyberspace domain are two very different types of conflicts which require separate strategies and different theories of victory. Wartime cyber conflict will touch all aspects of the wide-ranging Joint All Domain Operations (JADO). Because of the connected character of 21st century warfare, wartime cyber conflict has the potential to compromise mission assurance at a scale previously unfathomable and never before experienced. But it is finite and limited to the duration of traditional battle, whereas peacetime cyber aggression is persistent and indefinite, the two classic characteristics of a forever war. US and allied partners are currently engaged in substantially violent peacetime cyber aggression focused on critical civilian, military, and intelligence

targets. The major threat actor's salami tactics[2] of incremental degradation to critical civilian and military assets is likely a preparatory action to a forthcoming traditional armed conflict. But to relegate nation-state-perpetuated cyber aggression during peacetime to a less urgent priority is a mis-assessment of the current situation. Which cyberbattle should be prioritized: the peacetime cyber aggression currently underway or the inevitable wartime cyber conflict? To what extent are NATO allies responsible for engaging with common adversaries executing OCO primarily in the civilian sector? Or should limited resources be allocated toward preparing for wartime cyber conflict to avoid devastating, cascading consequences during battle? Without coordinated preparation for future battles, adversaries will undoubtedly pre-emptively embed in critical JADC2 systems. The Cyberspace domain provides remote access to the critical rear battle area and the ability to compromise critical JADC2 systems during battle with a proverbial single click. The NATO way of war relies heavily on joint-force interdependencies, which in turn rely on uncompromised critical digital data and communication systems. Compromise would greatly hinder NATO's force superiority.

The answer is less a matter of priority and more a matter of practicality. Can we do both? We can and we must. It is essential that NATO allies coalesce to agree upon strategy and impose conditions for conclusion to the current peacetime cyber aggression perpetuated by common adversaries, while simultaneously preparing a separate strategy for wartime cyber conflict.

Cyber conflict is a sustainable and effective form of power projection for all threat actors. The tactical asymmetry is in their favour: the cyber battlefield is pre-leveled, pitched battles are eschewed in favour of sporadic, targeted, surprise aggression, stockpiles are irrelevant, and advanced weapon systems are not required to achieve a catastrophic effect. The most advanced cyber defence technologies amount to little more than

cyber – Maginot Lines that can be and are regularly circumvented. Most important, adversary cyber campaigns reliably meet national-interest objectives within an acceptable cost-benefit calculation. The escalating frequency and sophistication of nation-state cyber campaigns is proof that adversaries view their military operations in Cyberspace as advantageous. Yet bearing the brunt of the current peacetime cyber aggression is not sustainable. This begs the question, what are the opportunities for response?

A Strategy for Cyberspace

The unfortunate trend, even in erudite national security circles, is to jump directly to a discussion of cyberweapons and their tactical use. Or strategic vagaries like 'impose costs' or 'collective defence' are presented as free-standing solutions to the very complicated problem of international cyber security. Sound military-strategic logic paradigm construction begins with the ends. What is it that we want to achieve and what are the combinations of ways and means required to achieve it? Strategy is not a list of actions to undertake or an acronym-laden vision statement. A cohesive strategy is a viable, sustainable overarching concept that connects actions to resources and strengths. The connections between ways and means in a well-crafted strategy will create a self-perpetuating momentum toward the specified desired end. The ends are where NATO partners need to begin. Once an end has been established and the relevant means and ways are identified, partners can allocate resources to effectively collapse the delta between available objectives and viable objectives.

Furthermore, this resource allocation must be supported by commitment and an alignment of incentives that ensure adherence to strategy execution. Few NATO partners have fully developed cyber conflict strategies with deterrence or cessation of cyber conflict as the desired ends. No

NATO member has developed or enacted a 10-, 20-, or 100-year cyber conflict strategy, despite indicators that suggest adversaries have done so.[3]

Cyberspace as an operational domain has many idiosyncratic features, but tedious discussion is not beneficial to allied strategists at this time. Legal discussion of what constitutes homeland, violence, aggression, or an attack in Cyberspace or thresholds for engagement when there is no body count can and will ensue for years. But it does not take years for focused cyber aggression to yield impact. Every day, the major threat actors exploit allied inaction and Cyberspace domain vulnerabilities to enrich themselves, degrade economic postures and warfighting capabilities while staying below the threshold for use of (kinetic) armed force.

Conclusion

No one would deny that a sovereign nation-state has the right to pursue their national interests. And no one can deny that focused attempts to disrupt, deny, and disable critical military C2 systems via cyber effects or combatant-focused espionage and reconnaissance falls within acceptable wartime behaviour. Simply put, when national interests and behaviours conflict with LOAC (Law of Armed Conflict) or Geneva Convention protocols in any domain, the behaviour in question is unacceptable. These jus en bello violations are an excellent starting point for defining the desired ends. The Tallinn Manual is an exemplary body of work which contains a comprehensive guide to current law and cyber operations. US and NATO allies would benefit from rapid adoption of policies on which there is consensus. LOAC and Geneva Convention protocols are not warfighting domain-specific. Agreement to uphold their tenets form the basis of their power. At minimum, US and NATO allies can resolve to recognize their precedence in the Cyberspace domain, as the Tallinn Manual astutely lays out.

The force with the most effective use of cyber weapons, tactics, techniques, and procedures to achieve their desired ends, will be the victor. Victory in cyber conflict has less to do with body count or Clausewitzian ideals of defeat or surrender, and more to do with achieving strategic objectives. For the two cyber conflict scenarios under consideration, victorious ends are diametrically opposed: Adversaries benefit from under-the-radar forever wars while allies benefit from subduing adversary aggression. For allies, victory will inevitably be tied to the application and enforcement of LOAC and Geneva Convention protocols in the Cyberspace domain, unilateral OCO/DCO (Defensive Cyber Operations) capabilities and an alignment of incentives to assure commitment to achieving mutually agreed upon desired ends. It is imperative that US and NATO allies make immediate, substantial steps toward cohesive deterrence strategies to disallow further damage imposed by the major threat actors. The major threat actors need only continue in their current strategy. Unabated, they are achieving their objective.

Ms Gentry Lane is the CEO and Founder of ANOVA Intelligence, an American defence tech company, and a Visiting Fellow at the National Security Institute at George Mason University's Antonin Scalia Law School. ANOVA's groundbreaking computational approach to anomaly detection is revolutionizing cyberwarfare engagement for US companies and allies globally.

Endnotes

1. Electronic warfare operations and/or violence in the Cyberspace domain perpetuated by criminal organizations are a different problem which require different resources and strategies to address.
2. Schelling, Thomas C., Arms and Influence, 'New Haven and London', Yale University Press, 2008.
3. Scobell, Andrew; Burke, Edmund J.; Cooper, Cortez A. III; Lilly, Sale; Ohlandt, Chad J. R.; Warner, Eric; Williams, J.D., 'China's Grand Strategy: Trends, Trajectories and Long-Term Competition', Santa Monica, California: RAND Corporation, 2020.