Evolving Operational Level Assessment of Cyberspace Operations and Cybersecurity

By Associate Professor Raymond Tortorelli, CISSP

US Naval War College

On 26 July 2018, US Cyber Command (USCYBERCOM) published a list of research topics that included the broad question, "How can we measure success and performance on the cyber battlefield?" As of 2018, doctrine apparently does not adequately address assessments of cyberspace operations (CO) at the operational level of warfare. In fact, the proposed Air Land Sea Application (ALSA) publication on Operations Assessments, as well as the assessments portions of JP 5-0, do not mention cyberspace at all. The Commander's Handbook for Assessment Planning and Execution mentions cyberspace only once in a quote referring to cyber as a domain. If assessments truly occur at all levels of warfare, as stated in the Commander's Handbook, then guidance should address all levels of warfare. Furthermore, there is a tendency to treat CO assessments the same as other assessments. While alike in many ways, there are major differences in the force's expertise level required to assess CO as well as the operational factors of time and space. An evolution of the people, processes and organization of the Maritime Operations Center (MOC) is required to properly inform doctrine on assessments in the cyberspace domain at the operational level of warfare.

Challenges in Cyberspace Assessments at the OLW

Operational art provides the linkage between tactics and strategy. The Russians have already applied the operational art to achieve strategic end states through CO in the Ukraine. However, offensive cyberspace operations (OCO) by the US are done in support of the Combatant Commander and assessment of those operations is typically done at the theater strategic level. As nation states like Russia continue to push the authority to conduct OCO to more operational and tactical units, the US is also delegating more authority for OCO. In time, component level commanders may be given tactical control of cyber mission forces (CMF) responsible for both offensive and defensive cyber operations (DCO). In addition, component level commanders share a responsibility for their own cybersecurity at the operational level of

warfare (OLW). Commanders must be able to assess the progress of a CO to accomplish an objective in time and space. However, *Joint Publication 3-12 for Cyberspace Operations* states that the "development of operational-level Measures of Performance/Measures of Effectiveness (MOPs/MOEs) for Cyberspace Operations is still an emerging aspect of operational art." [1]

OLW planners are concerned with developing objectives and desired effects to achieve those objectives. This results in tasks and tactical actions to assigned forces to achieve the desired effects. These actions should be definable and measurable both in terms of performance and effectiveness. Tactical actions feed the operational assessment, which in turn feeds a strategic assessment. Effects and task analysis provide a commander with measurable data, and a deficiency analysis of that data leads to recommendations to the commander. The commander then makes a decision, perhaps a re-attack in the case of a bomb that did not hit its mark. This cycle of monitor, evaluate and recommend is continually occurring to provide the commander with the most current assessment. The more rapid the assessment, the better the commander's situational awareness and the faster the commander's decision cycle. Ultimately, assessments exist to support the commander's decision-making. In the case of cyberspace operations and cybersecurity, these measures of performance (MOPs) and measures of effectiveness (MOEs) are often measured from outside the command and control of the requester, making it difficult for a Component Commander to assess his effectiveness across the operational functions and react as appropriate.

People, Processes and Organization Aiding in Cyberspace Operational Assessments

Although some cyberspace operations involve effects that can be observed over time, CO often happen at the speed of light, meaning time is as critical if not more critical than in other operations. The recent speed and rapid spread of the NotPetya attack to companies like Maersk and Merck demonstrates why current battle rhythms do not accommodate for future operations in the cyberspace domain. Lightning speed operations require lightning speed assessments. This can be achieved with better processes, new hardware and software tools, and the use of artificial intelligence (AI).

[1] Joint Publication 3-12 Cyberspace Operations. Joint Staff. 8 June 2018, IV-22

Measurements require multiple sources and integration. To measure the effectiveness of an offensive cyberspace attack meant to deny or degrade a computer network might require the attacker using a tool like a packet sniffer on the network to show a reduction in network traffic or signals intelligence (SIGINT) reporting communications to that effect. Intelligence support is also necessary throughout both planning and execution. A power disruption caused by OCO could be assessed through visual information of lights out or human intelligence (HUMINT) reporting. A combination of the above could be used to increase confidence of validation. Measuring CMF performance in the information environment might also require sources outside of the MOC's C2. As an example, imagine a tool developed by the CMF and their support team but implanted locally by operatives. In this case, cross service integration or even agency integration is desired. Processes for Information Exchange Requirements (IERs) between the Cyber Mission Forces (CMF), Cyberspace Operations - Integrated Planning Elements (CO-IPEs), Joint Force Headquarters – Cyber (JFHQ-C) and DODIN (JFHQ-DODIN), Joint Force Commanders and the MOC cyberspace planners and assessments planners must be codified and further developed at the OLW.

Getting subject matter expertise involved in assessments planning and execution has always been a fleet-wide problem. It is magnified with the cyberspace planner. Although this varies in practice from fleet to fleet, the Maritime Operations Center Standardization Manual calls for the assessments cell in the maritime component to consist of 5 staff, only one of which is required to attend the Joint Information Operations Planners Course. In addition, the Maritime Operations Center Standardization Manual calls for only one cyberspace planner. If during transition from peacetime to crisis operations, that cyberspace planner is attending the cyber fires and effects working group, cyber threat working group, NCCC meetings, C2 of C2 working group and the IO working group, where is there time left in the battle rhythm to attend the Maritime Assessments Working Group? There is an undesirable gap in the ability for the cyberspace planner to interface with the assessments cell. Not only should manning be increased to accommodate but current staff organization and battle rhythms must change to better accommodate for future assessments of cyberspace.

More on AI

In the end, this is all about getting the right information to the commander at the right time. The speed with which assessments and actionable recommendations are made is critical to winning the war. Human in the loop (HITL) has been the standard for assessments but progress requires adaptation to the times. In reality, HITL is often many humans in the loops. The fastest method to measure effects and performance is to have automated tools capable of capturing the effects and reporting back to the attacker in near real time. A tool that both gains access and reports it provides a valuable MOP. If an automated tool is combined with automated ISR and VI inputs, an immediate assessment can be made. Vice multiple humans, HITL can literally become a single well-trained man in the loop and the speed of an actionable recommendation to the commander is increased. As artificial intelligence and neural networks becomes more advanced and predominant, one can foresee a logical progression to a time when these tools can both assess and make recommendations directly to operations further removing the man in the loop.

Conclusion

The enemy is within our firewalls. To survive, the MOC concept must continue to evolve in the cyberspace domain. The key to solving the assessment problem is in developing and adopting a new model-driven paradigm requiring validation of the MOC, its missions, and the cyber-vulnerable systems supporting the mission. To keep ahead, a strategic vision of the MOC must include wargaming and developing doctrine for cyberspace operational assessments, in order to increase the speed of the commander's decision cycle. The Navy Warfare Development Center (NWDC) could lead this doctrine development using expertise from both the Navy Information Warfare Development Center (NIWDC) and Fleet Cyber Command.