

ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO INSTITUTO MEIRA MATTOS PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIAS MILITARES	
Curso:	Mestrado e Doutorado
Disciplina:	Poder Cibernético: Inovação, Absorção e Disrupção
Enquadramento:	Minicurso
Carga Horária:	15 horas (1 Crédito)
Docentes:	Dr. Breno Pauli Medeiros (Pós-Doutorando PPGCM)
Período letivo:	2024.2
Estrutura	
	<ul style="list-style-type: none"> • Distribuição da carga horária: (10h de leitura + 2x1h30min de palestra + 2h de avaliação = 15h): 2 palestras de 1h30 min de duração, precedidas pela leitura dos textos pelos alunos. 2h para avaliação • Avaliação: Os alunos irão escrever artigos de 500 a 1000 palavras. Os artigos mais promissores serão recomendados para publicação no OMPV. Os artigos devem ser enviados no prazo de 10 dias uteis após o término da última palestra. • Datas: 26/08 (segunda) e 28/08 (quarta). • Horário: Das 19h às 21h • Modelo: Online.
EMENTA	
	<p>Palestra 1 – Teoria: O conceito de Poder Cibernético e seus marcos de utilização.</p> <p>Bibliografia Palestra 1:</p> <ul style="list-style-type: none"> • Obrigatória – <ul style="list-style-type: none"> ○ MEDEIROS, Breno Pauli; GOLDONI, Luiz Rogério Franco. The Fundamental Conceptual Trinity of Cyberspace. Contexto Internacional, v. 42, p. 31-54, 2020. ○ SEGAL, Adam. The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age. Hachette UK, 2016. - Cap. 1. • Complementares – <ul style="list-style-type: none"> ○ KUEHL, Daniel T. From cyberspace to cyberpower Defining the problem. Cyberpower and national security, v. 1, 2009. ○ SEGAL, Adam. The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age. Hachette UK, 2016. - Cap. 2. ○ MOORE, Daniel. Offensive cyber operations: understanding intangible warfare. Hurst Publishers, 2022. – Cap. 5 e 6. ○ FITTON, Oliver. Cyber operations and gray zones: Challenges for NATO. Connections, v. 15, n. 2, p. 109-119, 2016.

Palestra 2 – Estratégia: Absorção e emprego do Poder Cibernético.

Bibliografia Palestra 2:

- **Obrigatória –**
 - DEVANNY, Joe; GOLDONI, Luiz Rogério Franco; MEDEIROS, Breno Pauli. The rise of cyber power in Brazil. **Revista Brasileira de Política Internacional**, v. 65, p. e013, 2022.
 - DEVANNY, Joe. Artificial Intelligence and Cyber Power: Foreign Policy Implications. Jack D. Gordon Institute for Public Policy. **Research Publications**. 63. 2024.
- **Complementares –**
 - BELLI, L. et al. **Governança da Cibersegurança no Brasil: Entender o passado, esclarecer o presente e construir o futuro**. [s.l.] FGV Direito Rio, 14 jun. 2024. Disponível em: <<https://cyberbrics.info/governanca-da-ciberseguranca-no-brasil-entender-o-passado-esclarecer-o-presente-e-construir-o-futuro/>>. Acesso em: 14 jun. 2024.
 - LONERGAN, E. D.; SCHNEIDER, J. The Power of Beliefs in US Cyber Strategy: The Evolving Role of Deterrence, Norms, and Escalation. **Journal of Cybersecurity**, v. 9, n. 1, p. tyad006, 5 jan. 2023.
 - HARKNETT, R. J.; FISCHERKELLER, M. P.; GOLDMAN, E. O. U.K. National Cyber Force, Responsible Cyber Power, and Cyber Persistence Theory. Disponível em: <<https://www.lawfareblog.com/uk-national-cyber-force-responsible-cyber-power-and-cyber-persistence-theory>>. Acesso em: 25 abr. 2023.
 - HARKNETT, R. J.; SMEETS, M. Cyber campaigns and strategic outcomes. **Journal of Strategic Studies**, v. 45, n. 4, p. 534–567, 7 jun. 2022.
 - MOORE, D. The Russian Spectrum of Conflict. Em: MOORE, D. (Ed.). **Offensive Cyber Operations**. 1. ed. [s.l.] Oxford University Press, 2022. p. 145–174.