

ESCOLA SUPERIOR DE GUERRA

PROJETO PEDAGÓGICO



CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA

Aprovado em ____ de ____ de 2026

Alexandre Oliveira Cantanhede Lago
General de Divisão Alexandre Oliveira CANTANHEDE Lago
Comandante da Escola Superior de Guerra

SUMÁRIO

• SÍNTESE HISTÓRICA	01
○ APRESENTAÇÃO	01
○ METODOLOGIA DE ENSINO DA ESG	02
○ ASPECTOS NORMATIVOS	05
• APRESENTAÇÃO DO CURSO	06
○ OBJETIVO GERAL	06
○ DIRETRIZES GERAIS	06
○ QUADRO GERAL DE CARGA HORÁRIA	10
• APÊNDICE AI ESTRUTURA CURRICULAR	12
○ ESTRUTURA CURRICULAR DO CSSDC	13
• APÊNDICE AII CRONOGRAMA DE ESTUDOS	18
○ CRONOGRAMA DE ESTUDOS CSSDC	19
• APÊNDICE AIII PLANO DE DISCIPLINAS	21
○ PLANO DE DISCIPLINA CSSDC	22

SÍNTESE HISTÓRICA

APRESENTAÇÃO

A Escola Superior de Guerra (ESG), criada pela Lei nº 785 de 20 de agosto de 1949 é um Instituto de Altos Estudos de Política, Estratégia e Defesa, integrante da estrutura do Ministério da Defesa, e destina-se a desenvolver e consolidar os conhecimentos necessários para o exercício das funções de direção e assessoramento superior na Administração Pública e para o planejamento da Segurança e da Defesa Nacionais, nela incluídos os aspectos relativos ao desenvolvimento nacional.

A ESG funciona como Instituição de Ensino Superior, atuando como centro de permanente de estudos, de pesquisas e de desenvolvimento e capacitação de recursos humanos sobre pensamento de defesa.

A Escola planeja, coordena e desenvolve os cursos instituídos pela Chefia de Educação e Cultura (CHEC) do Ministro de Estado da Defesa e atua, na organização do debate entre as lideranças civis e militares a respeito das questões da defesa, contribuindo para aumentar o envolvimento da sociedade brasileira nos assuntos da defesa nacional.

Na organização dos cursos são considerados os seguintes princípios:

- ✓ a relação indissociável entre ensino e pesquisa;
- ✓ a transdisciplinaridade do conhecimento;
- ✓ o pensamento crítico e abrangente;
- ✓ o pluralismo de ideias;
- ✓ a integração entre diferentes órgãos da Administração Pública;
- ✓ a interação entre civis e militares;
- ✓ a correlação e a integração dos estudos individuais;
- ✓ a valorização da experiência do estagiário;
- ✓ a compreensão da conjuntura nacional e internacional;
- ✓ a promoção do assessoramento de alto nível; e
- ✓ a garantia do padrão de qualidade.

Para tanto, promove estudos e pesquisas, compreendendo o ensino, a extensão e o intercâmbio de conhecimentos, por meio de Cursos, Simpósios, Ciclos de Estudo, dentre outras atividades acadêmicas.

As atividades de estudo e ensino desenvolvidas são coordenadas e conduzidas pelo Departamento de Estudos, a quem cabe, ainda, desenvolver outras atividades finalísticas por intermédio dos Institutos e Centros integrantes da estrutura regimental da ESG.

As suas diretrizes pedagógicas, centradas em valores humanos e sociais, promovem estudos integrados e participativos, de natureza exclusivamente acadêmica. Com foco na melhoria contínua, aperfeiçoa constantemente suas atividades pedagógico-institucionais.

A ESG desenvolve as suas atividades na Fortaleza de São João – Av. João Luiz Alves, s/nº - Urca, Rio de Janeiro, RJ, CEP 22291-090. Mais esclarecimentos podem ser obtidos por meio dos tel. (21) 3545-9869, (21) 3545-9889 ou pela navegação na página oficial da ESG na internet www.esg.br, onde estão disponíveis informações sobre o histórico da Escola, seus diversos cursos e demais atividades desenvolvidas.

METODOLOGIA DE ENSINO DA ESG

A metodologia de ensino da ESG busca propiciar, para todos os cursos, fundamentação teórica, compreensão de conjunturas em uma abordagem sistêmica e domínio de instrumento para análise coletiva da realidade, com vista à elaboração de políticas e estratégias de ação e à sistematização coletiva e individual de conhecimentos. Os matriculados na ESG são denominados como estagiários, visando estimular a perspectiva de aplicação e vivência dos conhecimentos adquiridos durante os diversos cursos por eles realizados.

Na ESG, o aporte teórico relevante das áreas de conhecimento é abordado evitando-se a adoção de verdades absolutas, sendo apresentadas múltiplas e diferentes visões sobre os assuntos tratados, de modo a incentivar o debate e o pensamento crítico e abrangente. São também propostas atividades de estudos e pesquisa de modo a ampliar a compreensão da realidade nacional e internacional.

- **A relação indissociável entre ensino e pesquisa.**

A pesquisa é responsabilidade inerente daquele que ensina, sendo uma oportunidade para o professor-pesquisador se manter em contínuo desenvolvimento quanto ao conteúdo, aos métodos de pesquisa e à compreensão da realidade. Por essa razão, a ESG valoriza o desenvolvimento permanente dos seus integrantes, assim como apoia e incentiva as iniciativas de autodesenvolvimento e a participação dos mesmos em eventos acadêmico-científicos, em grupos de pesquisa e em todas as atividades que favoreçam a capilarização dos conhecimentos construídos, contribuindo para as atividades docentes junto aos estagiários dos cursos.

- **O conhecimento é inter e transdisciplinar.**

Altos estudos envolvem a capacidade de discernir o contexto, o global, o multidimensional e a interação complexa dos elementos (MORIN, 2000). A estruturação curricular da ESG busca uma organização do conhecimento como uma teia ou rede orgânica de acesso livre. O recorte teórico dos conhecimentos busca ultrapassar as barreiras tradicionais dos conteúdos disciplinares visando, não “o domínio sobre várias outras disciplinas, mas a abertura de todas elas àquilo que as atravessa e as ultrapassa (...)” (UNESCO, 1994).

O pensamento complexo é também incentivado nas atividades de interpretação, análise, crítica e planejamento estratégico de macro contextos desenvolvidos nos cursos, por meio dos trabalhos, em grupo e individuais, com temas transversais que objetivam articular a contribuição das diversas áreas para integrar e aprofundar os conhecimentos estudados.

- **O conhecimento, como bem cultural imaterial, é construído, reconstruído e interpretado social e coletivamente. Os saberes culturais são apropriados e transformados a partir da atividade mediada.**

A ESG adota, em sua prática didático-pedagógica, a base teórica sociointeracionista, considerando que as funções ou processos mentais superiores e tipicamente humanos têm origem social (VYGOTSKY, 1992). A construção de conhecimento e a aprendizagem humana acontecem fundamentalmente pelos processos de interação e mediação nas relações entre o indivíduo e o mundo exterior, num processo histórico e social. Por essa razão, todos os cursos da ESG promovem atividades de estudos em grupo (pesquisa, análise e sistematização de conhecimentos conjunta), primando pela oportunidade de troca de experiências, de intercâmbio de informações e de diferentes

visões de mundo. O corpo docente da ESG assume o papel de mediação no processo de interlocução das atividades realizadas, atuando de forma interdisciplinar. Dessa forma, as atividades de estudos são estruturadas de modo a propiciar:

- compreensão do Poder Nacional;
- conhecimentos teóricos básicos;
- análise de conjunturas, por meio de exposições de conferencistas ilustres, como autoridades acadêmicas e governamentais em diversas esferas, e representantes de inúmeras instituições;
- compreensão *in loco* das questões centrais abordadas em cada curso, realizada por meio de viagens e visitas de estudo; e
- sistematização de conhecimentos por meio de trabalho final de curso como forma de sistematizar os saberes construídos socialmente.

As palestras e conferências são preferencialmente precedidas por estudo prévio de material teórico de referência no assunto, indicado pelas Divisões de Estudo. Os fundamentos teóricos são seguidos de análises conjunturais que permitem a integração da teoria com a prática e com a realidade, seja por meio de debates, discussões dirigidas, trabalhos em grupo, estudos individuais, visitas ou viagens.

A prática avaliativa adotada objetiva acompanhar o processo de produção intelectual dos estagiários a partir dos objetivos propostos e dos critérios estabelecidos em cada curso. Um dos princípios norteadores da prática avaliativa na ESG é o acompanhamento da produção coletiva e individual, buscando uma análise global e transdisciplinar, tendo em vista que os trabalhos são elaborados como uma articulação dos conhecimentos trabalhados nas diferentes fases de cada curso.

Os procedimentos avaliativos e as condições de aprovação estão pautados em documentos e orientações normativas da ESG. Os registros avaliativos acontecem na forma de conceitos, sem o objetivo de classificação entre os estagiários, de modo a fomentar a apreciação das produções por parte dos avaliadores e reorientá-las, se for o caso.

A avaliação do ensino é realizada por meio da contribuição dos estagiários que analisam as atividades curriculares, em consonância com o objetivo das disciplinas, bem como os responsáveis por estas atividades.

Deste modo, diante de um contexto global marcado por desafios multifacetados, que exigem uma abordagem interdisciplinar e crítica, a ESG se propõe a oferecer uma educação que não apenas transfira conhecimentos, mas que desenvolva o pensamento estratégico, a liderança e a capacidade de atuação em ambientes dinâmicos e desafiadores.

O presente Projeto Pedagógico busca consolidar os esforços educacionais e administrativos, alinhando as práticas pedagógicas às diretrizes estratégicas de desenvolvimento, de segurança e de defesa do Brasil, promovendo a excelência acadêmica e a formação integral.

ASPECTOS NORMATIVOS

Em consonância com os documentos normativos pertinentes, anualmente, é publicada a Diretriz para o Planejamento e a Execução das Atividades de Estudo, Pesquisa, Ensino, Pós-Graduação, Extensão e Processo Seletivo dos Cursos da Escola Superior de Guerra (ESG) e da Escola Superior de Defesa (ESD).

Para o ano letivo de 2026, a referida diretriz está aprovada pela Portaria AED-MD Nº 48, de 06 de janeiro de 2026.

A partir deste documento e, conforme as competências estabelecidas no Regimento Interno da ESG, são desenvolvidos, pelos Setores responsáveis, os processos de capacitação que propiciam o cumprimento da missão institucional da ESG.

APRESENTAÇÃO DO CURSO

DURAÇÃO: 14 SEMANAS

CARGA HORÁRIA TOTAL: 460 H/A

1 OBJETIVO GERAL

O Curso Superior de Segurança e Defesa Cibernética (CSSDC) destina-se a preparar integrantes da Administração Pública, estadual e municipal, militares das Forças Armadas, das Polícias Estaduais e Corpos de Bombeiros Estaduais, representantes de nações amigas e profissionais da iniciativa privada, para o assessoramento político-estratégico, considerando os conceitos e os fundamentos da segurança e da defesa cibernéticas.

2 DIRETRIZES GERAIS

2.1 Estruturação

O curso é desenvolvido no formato híbrido, com as atividades de ensino presencial e não presencial.

Para a consecução do objetivo geral do curso, a estrutura curricular é disposta com base na Trilha do Conhecimento em Cibernética, elaborada pelo Comando de Defesa Cibernética e baseada em currículo apoiado em competências, que refletem a abordagem metodológica do curso.

Os conteúdos estão organizados por disciplinas que apresentam fundamentos e conceitos básicos, estudos de casos, análise, planejamento e exercícios de decisão estratégica e de simulação de crise cibernética, que constituem os módulos da Trilha do Conhecimento.

A estrutura curricular do curso oferta 8 disciplinas básicas, de caráter obrigatório.

As disciplinas são organizadas em 3 blocos de disciplinas: Fundamentação Político-Estratégica; Dimensão Cibernética e Segurança da Informação; e Fundamentação para Pesquisa Científica em Cibernética.

O estagiário aprovado em todas as disciplinas do curso recebe o Certificado de Conclusão do Curso com o nível de ensino de Pós-Graduação Lato Sensu de Especialização em Políticas e Estratégias Cibernéticas.

O curso contempla a realização de trabalhos em grupo, que consistem na elaboração de análises da conjuntura atual e de cenários prospectivos envolvendo crises

e conflitos, relacionados aos conhecimentos adquiridos ao longo do curso, com questões de interesse da cibernética no âmbito da Defesa Nacional e das instituições.

Os procedimentos acadêmicos são pautados pela interação entre os estagiários, de forma a propiciar o trabalho em grupo e a integração dos conhecimentos.

Para o cômputo de carga horária do curso são considerados:

- ensino não presencial: 15 (quinze) horas/aula semanais, de 2ª a 6ª feira, com 3 (três) tempos diários, de 40 minutos cada;

- ensino presencial: 37 (trinta e sete) horas/aula semanais, com 8 (oito) tempos diários de 40 minutos cada, sendo 5 (cinco) pela manhã e 3 (três) na parte da tarde, de 2ª a 5ª feira e 5 (cinco) pela manhã, nas 6ª feiras.

As atividades específicas de ensino do CSSDC ocorrem ao longo de 14 (quatorze) semanas, sendo 4 semanas de ensino não presencial e 10 semanas de ensino presencial, iniciando em 27 de julho e terminando em 06 de novembro, possuindo carga horária de 398 h/a, referentes, estritamente, às atividades de ensino (disciplinas e atividades de Complementação do Ensino e de Estudos e Pesquisas Individuais).

Os estagiários podem participar de outras atividades acadêmicas de caráter complementar, como participação em encontros e seminários, quando ocorrerem nas tardes das sextas-feiras.

Está prevista uma semana de intervalo entre as atividades de ensino de ensino não presencial e de ensino presencial, computada como atividade administrativa do Curso, destinada ao deslocamento e instalação do estagiário na cidade do Rio de Janeiro.

Considerando o disposto na Portaria Normativa Interministerial MD/MEC nº 3.867, de 14 de julho de 2022 e na Resolução CES/CNE nº 4, de 16 de julho de 2021, o curso é equivalente aos cursos de pós-graduação lato sensu de especialização, conforme definido na Resolução nº 1 CNE/CES, de 6 de abril de 2018, da Câmara de Educação Superior do MEC, alterada em seu art. 11 pela Resolução nº 4/CNE/CES, de 16 de julho de 2021.

A especificidade de determinados assuntos do Curso poderá acarretar a necessidade de apoio de outras organizações por meio de Pedidos de Cooperação de Ensino (PCE) e de outros instrumentos.

2.2 Atividades Complementares aos Estudos

São previstas atividades que se ligam, direta ou indiretamente, às disciplinas do Curso. Tais atividades englobam os Estudos Interdisciplinares de Campo (EIC), que contemplam Viagem de Estudo (VG) e Visita Técnica (VT), a setores de interesse do Curso.

As horas destinadas aos EIC estão contidas nas cargas horárias da disciplina de Atividades Cibernéticas.

Serão realizadas 1 (uma) VG em território nacional e 1 (uma) VT na cidade do Rio de Janeiro.

Os EIC constituem um dos meios de aprendizagem mais eficazes, contribuindo para o enriquecimento do conteúdo programático, uma vez que propiciam um maior aprofundamento do conhecimento de áreas político-estratégicas de interesse da cibersegurança e da ciberdefesa, além de promover uma maior integração entre diversos órgãos e a interação entre civis e militares. Tais eventos permitem, se necessário, o fracionamento dos grupos para diferentes atividades ao mesmo tempo e sua posterior junção para discussão dos dados colhidos. Em consequência, poderão, a critério do Diretor do Curso, ser planejados tempos para trabalho em grupo durante as viagens, de modo a consolidar os conhecimentos auferidos, bem como ser solicitado um relatório aos diversos grupos de trabalho.

2.3 Avaliação da Aprendizagem

2.3.1 Das Disciplinas

Haverá avaliação da aprendizagem dos estagiários em todas as disciplinas, sendo utilizados diferentes instrumentos/técnicas neste processo, de acordo com o previsto no Documento Técnicas e Instrumentos de Avaliação da Aprendizagem (D5).

A avaliação poderá ser desenvolvida individualmente, em duplas ou em grupos maiores.

2.3.2 Das Atividades Avaliativas Integradoras

Os estagiários deverão elaborar seis atividades avaliativas integradoras, com seus respectivos entregáveis, ao longo do curso: um Trabalho Acadêmico no formato de Ensaio Acadêmico (EA) e cinco Exercícios de Decisão Estratégica (EDE), conforme descrição abaixo:

A- Trabalho Acadêmico

O estagiário deverá elaborar, individualmente, um Ensaio Acadêmico (EA), ao longo do curso, com o tema relacionado com as disciplinas curriculares e com base na disciplina Metodologia da Pesquisa Científica.

O EA tem por finalidade registrar e sistematizar a contribuição do estagiário, mediante a articulação entre sua experiência profissional e os conhecimentos adquiridos no CSSDC.

A elaboração dar-se-á de forma processual, conforme etapas, prazos e apresentação oral definidos em Cronograma de Trabalho, sob orientação de docentes designados pelo Departamento de Estudos (DE), observadas as diretrizes das aulas de Metodologia da Pesquisa e do Manual para Elaboração de Trabalhos Acadêmicos da ESG.

B- Exercícios de Decisão Estratégica

Os EDE focam o relacionamento da teoria e do conhecimento com a aplicação prática, considerando as condicionantes fictícias ou reais. Esses exercícios não buscam apenas a "resposta certa", mas sim o desenvolvimento do pensamento crítico e da capacidade analítica.

O cerne dessa prática é desenvolver competências críticas em ambientes incertos, típicos do ciberespaço e da geopolítica moderna, fomentando habilidades como análise de inteligência, priorização de riscos e formulação de políticas.

Os estagiários, distribuídos em grupos de trabalho, recebem um documento que apresenta um cenário fictício, detalhando um dilema real, uma situação de ameaça, de risco ou de crise e são instigados a apresentar soluções multifacetadas.

O Curso submete os estagiários a cinco EDE, a saber:

- VIGIA;
- KRAKEN;
- GEOCIBERFIN;
- CIBERPOL;
- CIBERINFRA;

2.3.3 Mensuração da avaliação da aprendizagem

Os procedimentos avaliativos estão pautados em documentos e orientações normativas próprias.

A avaliação é expressa em conceitos, com base no registro avaliativo de acordo com a tabela abaixo. O conceito será registrado no histórico escolar.

REGISTRO AVALIATIVO	CONCEITO	RESULTADO	SITUAÇÃO DO ESTAGIÁRIO
10.0 – 9.0	A	Excelente	Aprovado
8.9 – 8.0	B	Muito Bom	
7.9 – 7.0	C	Bom	
Abaixo de 7.0	D	Insuficiente	A ser apreciada pelo Diretor de Estudos, ouvido o Conselho de Ensino.

2.3.2 Avaliação do Ensino

É realizada a partir de informações coletadas em Fichas de Avaliação preenchidas pelos estagiários, visando identificar e analisar os aspectos positivos e as necessidades de mudança no que tange à proposta curricular, ao desenvolvimento do curso e ao desempenho dos integrantes da ESG, bem como dos convidados ligados às atividades de ensino.

2.4 Frequência às Atividades

A frequência às atividades programadas, acadêmicas e outras, é obrigatória. Os critérios relativos ao controle da frequência, motivo da falta, cancelamento da matrícula e desligamento do curso estão definidos em Orientação Normativa própria.

Os estagiários devem envidar esforços para evitar faltar às atividades acadêmicas previstas, considerando a oportunidade de contribuírem com seus conhecimentos profissionais para o desenvolvimento dos temas abordados.

O comparecimento dos Estagiários das nações amigas às Atividades Complementares e determinadas atividades de estudo ficará a cargo do Diretor do Curso.

3 QUADRO GERAL DE CARGA HORÁRIA

Atividade	Carga-Horária (h/a)
De Estudos	389
Complementação do Ensino	07
Estudos e Pesquisas Individuais	32
Administrativas	32
Carga Horária Total	460

Apêndices:

A - I – CSSDC (Estrutura Curricular)

A - II – CSSDC (Cronograma de Estudos)

A – III – CSSDC (Plano de Disciplinas)

APÊNDICE AI

ESTRUTURA CURRICULAR



MINISTÉRIO DA DEFESA
ESCOLA SUPERIOR DE GUERRA
DEPARTAMENTO DE ESTUDOS
DIVISÃO DE ASSUNTOS DE CIÊNCIA E TECNOLOGIA
Curso Superior de Segurança e Defesa Cibernética (CSSDC)
ESTRUTURA CURRICULAR GERAL

DISCIPLINA		CARGA HORÁRIA
FUNDAMENTAÇÃO POLÍTICO-ESTRATÉGICA		
I	Política e Espaço Cibernético	35
II	Geopolítica do Espaço Cibernético	26
III	Estratégia do Espaço Cibernético	56
IV	Relações Internacionais e Espaço Cibernético	20
V	Marcos Normativos do Espaço Cibernético	40
SEGURANÇA DA INFORMAÇÃO E DIMENSÃO CIBERNÉTICA		
VI	Segurança da Informação e Proteção de Dados	49
VII	Atividades Cibernéticas	139
FUNDAMENTAÇÃO PARA PESQUISA EM CIENTÍFICA		
VIII	Metodologia da Pesquisa Científica	27

ESTRUTURA CURRICULAR POR DISCIPLINA

I - POLÍTICA E ESPAÇO CIBERNÉTICO – 35 h		
CONTEÚDO: Aspectos Fundamentais da Conjuntura Política e Espaço Cibernético – 35 h		
UNIDADE DE ESTUDO		CH
1	Política e Poder - Teorias do Poder	3
2	Poder Nacional e Teorias de Estado	3
3	Política Contemporânea e Espaço Cibernético	3
4	Política, Sociedade e Parceria Público Privada na Dimensão Cibernética	3
5	Poder Nacional e Objetivos Nacionais	3
6	Política Nacional e o Poder Cibernético Nacional	2
7	Estratégia Nacional e a Dimensão Cibernética	2
8	Segurança e Defesa Nacionais e a Dimensão Cibernética	3
9	Expressões do Poder Nacional	3
10	Fenomenologia do Terrorismo	3
11	Fundamentos da Ciberpolítica	3
12	Relação entre Ciberpolítica, Geopolítica, Estratégias dos Estados, Marcos Normativos de Cibernética e Relações Internacionais	2
13	Avaliação da Aprendizagem	2

II - GEOPOLÍTICA DO ESPAÇO CIBERNÉTICO – 26 h		
CONTEÚDO: Estudo Geopolítico de Áreas Estratégicas - 6		
UNIDADE DE ESTUDO		CH
1	Áreas Estratégicas	3
2	Panorama Geopolítico	3
CONTEÚDO: Estudos Geopolíticos Aplicados ao Espaço Cibernético – 11 h		
UNIDADE DE ESTUDO		CH
3	Paradigmas da Geopolítica Mundial, Ciberespaço e Soberania Nacional	8
4	Conhecimento e Geopolítica do Espaço Cibernético. Espaço cibernético como vetor estratégico da estruturação em rede da sociedade	3
CONTEÚDO: Geopolítica do Século XXI e Espaço Cibernético – 09 h		
UNIDADE DE ESTUDO		CH
5	Panorama Geopolítico Contemporâneo e o Espaço Cibernético – A formulação de uma Grande Estratégias Nacional na Era da Cibernética e do Lawfare	5
6	Postura geopolítica, espaço cibernético e a condição pós-westfaliana	2
7	Avaliação da Aprendizagem	2

III - ESTRATÉGIA DO ESPAÇO CIBERNÉTICO – 56 h		
CONTEÚDO: Aspectos Fundamentais da Conjuntura e Espaço Cibernético – 56 h		
UNIDADE DE ESTUDO		CH
1	Evolução do pensamento estratégico	3
2	Estratégias internacionais relacionadas com a dimensão cibernética	2
3	Teoria de crise	8
4	Espaço cibernético como vetor estratégico da estruturação em rede da sociedade	2
5	Atividades cibernéticas e computação quântica	3
6	Estudo de casos históricos de ataques cibernéticos	15
7	Exercício de decisão estratégica (CIBERPOL)	21
8	Avaliação da Aprendizagem	2

IV - RELAÇÕES INTERNACIONAIS E ESPAÇO CIBERNÉTICO – 20 h		
CONTEÚDO: Aspectos Fundamentais das Relações Internacionais e Espaço Cibernético – 20 h		
UNIDADE DE ESTUDO		CH
1	Teoria das Relações Internacionais e espaço cibernético	4
2	Fundamentos do Direito Internacional e Direitos Humanos no espaço cibernético	4
3	Ciberdiplomacia	2
4	Impactos das atividades cibernéticas na agenda de paz e segurança	2
5	Posicionamentos e iniciativas diplomáticas no cenário internacional no âmbito do espaço cibernético	6
6	Avaliação da Aprendizagem	2

V - MARCOS NORMATIVOS E ESPAÇO CIBERNÉTICO – 40 h		
CONTEÚDO: Marcos Normativos Aplicados ao Espaço Cibernético – 40 h		
UNIDADE DE ESTUDO		CH
1	Marcos Normativos Internacionais e Nacionais Aplicados ao Espaço Cibernético, à Política, à Estratégia e à Defesa	27
2	Cibercrimes e Legislação Penal	2
3	Marcos Normativos de Gestão Forense Aplicável ao Espaço Cibernético - Obtenção e Aplicação Judiciária de Evidências Forenses Cibernéticas	2
4	Normas para Preservação de Evidências em Crimes Digitais	2
5	Marcos Normativos do Ministério da Defesa Aplicável ao Espaço Cibernético	5
6	Avaliação da Aprendizagem	2

VI - SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS – 49 h		
CONTEÚDO: Segurança da Informação e Espaço Cibernético – 49 h		
UNIDADE DE ESTUDO		CH
1	Fundamentos de segurança da informação	12
2	Lei Geral de Proteção de Dados (LGPD)	8
3	Ambiente Informacional Digital	10
4	Segurança na internet	17
5	Avaliação da Aprendizagem	2

VII - ATIVIDADES CIBERNÉTICAS – 139 h		
CONTEÚDO: Fundamentos do Espaço Cibernético – 16 h		
UNIDADE DE ESTUDO		CH
1	Conceitos e fundamentos de cibersegurança e ciberdefesa	16
CONTEÚDO: Inteligência e Ameaça Cibernética – 24 h		
UNIDADE DE ESTUDO		CH
2	Inteligência cibernética	24
CONTEÚDO: Cultura Cooperativa na Dimensão Cibernética – 8 h		
UNIDADE DE ESTUDO		CH
3	Integração e cooperação interagências no campo do ciberespaço	8
CONTEÚDO: Crise Cibernética – 15 h		
UNIDADE DE ESTUDO		CH
4	Teoria e gerenciamento de crises cibernéticas	15
CONTEÚDO: Atividades do Ministério da Defesa e Espaço Cibernético – 30 h		
UNIDADE DE ESTUDO		CH
5	Inferência do ciberespaço nas atividades do Ministério da Defesa e FFAA	30
CONTEÚDO: Atividades de Espaço Cibernético – 46 h		
UNIDADE DE ESTUDO		CH
6	Estudo Interdisciplinar de Campo I	16
7	Estudo Interdisciplinar de Campo II	4
8	Exercício de decisão estratégica de crise cibernética em infraestrutura crítica (CIBERINFRA)	24
9	Avaliação da Aprendizagem	2

VIII - METODOLOGIA DA PESQUISA CIENTÍFICA – 27 h		
CONTEÚDO: Coleta, Tratamento e Análise dos Dados – 27 h		
UNIDADE DE ESTUDO		CH
1	Técnicas e análises	7
2	Trabalho Acadêmico	20

ATIVIDADES COMPLEMENTARES– 56 h		
ATIVIDADES		CH
1	Administrativas	32
2	Complementação do Ensino	07
3	Estudos e Pesquisas Individuais	24
4	Estudo Interdisciplinar de Campo I - Viagem de Estudos	(*)
5	Estudo Interdisciplinar de Campo II - Visita de Estudos	(*)

OBSERVAÇÕES:

(*) – carga horária já computada na disciplina Atividades Cibernéticas.

(**) – será normal ocorrer alterações nas unidades de estudos e nas cargas horárias.

APÊNDICE AII

CRONOGRAMA DE ESTUDOS

CRONOGRAMA GERAL DE DISCIPLINAS DO CURSO SUPERIOR DE SEGURANÇA E DE

MÊS	JULHO					AGOSTO				
MODALIDADE	ATIVIDADE NÃO PRESENCIAL									
SEMANA	1ª		2ª		3ª		4ª			
DIA	27 31		03 07		10 14		17 21			
2ª Feira	Orient Dir Curso		II-2	Pan Geop	VI-1	Fund Seg Info	VII-1-3	Cpcd Op Ciber		
3ª Feira	I-1	Teoria Poder	II-3	Pard Glob & Ciber	VI-1		VII-1-4	Atores Ciber Mal		
4ª Feira	I-2	Poder Nac	III-1	Evol Pen Estr	VI-1		VII-1-5	Ameaças Ciber		
							VII-1-6	Atq Ciber		
5ª Feira	I-5 / I-9	Obj Nac Exp P Naci	IV-1	Teo RI & Ciber	VII-1-1	Fund Espaço Ciber	VII-1-7	Aç Trr Ciber		
6ª Feira	II-1	A Estr	V-1	M Norm	VII-1-2	Def Elm Parad Ciber	VIII-1	Tec e Anl Psq		
	Orient Dir Curso									

MÊS	AGOSTO		SETEMBRO							
MODALIDADE										
SEMANA	5ª			6ª			7ª			
DIA	3104		0711			1418		21		
2ª Feira	Mdd Adm - Recepção Conhecendo a ESG-ARI Mdd Adm-CPC/DTIC/Bibliot Orientação Geral-ASPIAvE Visita Instalações-CPC			FERIADO NACIONAL			III-5 III-5 III-5 III-5	Atv Ciber e Comp Quântida	VII- 2.6.8.11 VII-5.12 VII-5.12 VII-5.12	
	Desv Interpessoal-ASPIAvE Desv Interpessoal-ASPIAvE Desv Interpessoal-ASPIAvE						II-3 II-3 II-3		Pdigma Geopol Mundial, Ciber/Soberania Naci	VII-2.2 VII-2.4 VII-2.5
3ª Feira	I-3	Pol Cont & Ciber	V-1 VI-2	LGPD			V-2	Crimes Ciber Leg Penal	VII-2.9	
	I-3	Pol Cont & Ciber	V-1 VI-2	LGPD			V-2		VII-2.13	
	I-4	Pol Soc PPP & Ciber	V-1 VI-2	LGPD			V-3		VII-5.1	
	I-4	Pol Soc PPP & Ciber	V-1 VI-2	LGPD			V-3		VII-5.2	
	I-7	Estrt Nac & Ciber	V-1 VI-2	LGPD			V-4		VII-5.3	
	II-2	Par Geopol & Cibe	V-1 VI-2	LGPD			V-4	Crimes Ciber Leg Penal	VII-5.4	
4ª Feira	Solenidade de Abertura		II-3	Paradigmas da Geopolítica Mundial, Ciberespaço e Soberania Nacional - Exercício			VI-3	Amb Infor Dig	VI-4	
	Aula Magna		II-3				VI-3		VI-4	
	VIII-1	Trabalho Acadêmico	II-3				III-6		Estudo casos Atq Ciber	VI-4
	VIII-1	Trabalho Acadêmico	II-3				III-6		Estudo casos Atq Ciber	VI-4
5ª Feira	VIII-1	Trabalho Acadêmico	II-6	Postura geopolítica, espaço cibernético e a condição pós- westfaliana			III-6	Estudo casos Atq Ciber	VI-4	
	VIII-1	Trabalho Acadêmico	II-6				III-6	Estudo casos Atq Ciber	VI-4	
	VIII-1	Trabalho Acadêmico	II-6				III-6	Estudos casos Atq Ciber	VI-4	
	I-8	Seg & Def Nac & Ciber	IV-2	Rel Intern & Ciber			III-6	Estudo casos Atq Ciber	VII-4.6	
	I-8	Seg & Def Nac & Ciber	IV-2	Rel Intern & Ciber			III-6	Estudo casos Atq Ciber	VII-4.6	
	I-11	Fund Ciberpolítica	IV-2	Rel Intern & Ciber			III-6	Estudo casos Atq Ciber	VII-2	
	I-11	Fund Ciberpolíticar	IV-2	Rel Intern & Ciber			III-6	Estudo casos Atq Ciber	VII-2	
	I-11	Fund Ciberpolítica	IV-3	Rel Intern & Ciber			III-6	Estudo casos Atq Ciber	VII-2	
6ª Feira	I-12	Ciberpolítica & Geo	IV-3	Rel Intern & Ciber			III-6	Estudo casos Atq Ciber	VII-2.9	
	I-12	Ciberpolítica & Geo	IV-4	Rel Intern & Ciber			III-6	Estudo casos Atq Ciber	VII-2.9	
	I-12	Ciberpolítica & Geo	IV-4	Rel Intern & Ciber			III-6	Estudo casos Atq Ciber	VII-2.9	
	II-2	Formulação de Grd Estrt Nacina Era Ciber e Lawfare	IV-5	Rel Intern & Ciber			I, II, III, IV e V	Aval - Apres GT	VII-2	
II-2		IV-5	Rel Intern & Ciber			Aval - Apres GT		VII-2		
II-2		IV-5	Rel Intern & Ciber			Aval - Apres GT		VII-2		
II-3	Pdigma Geopol Mundial, Ciber/Soberania Naci	IV-5	Rel Intern & Ciber			Aval - Apres GT		VII-2		
6ª Feira	II-3		IV-5	Rel Intern & Ciber				Aval - Apres GT	VII-2	
	Estudos e Pesquisas Individuais (EPI)									

EXERCÍCIO GUARDIÃO CIBERNÉTICO SEMANA 21 A 25 SET

OUTUBRO					OUTUBRO / NOVENBRO				
10ª	11ª			12ª		13ª		14ª	
09	12 16			19 23		26 30		02 06	
Mét detecção Mét detecção Anl Vul ciber Hacktivismo Prev ameaças Ciber PEstrt FFAA D Ciber MB PEstrt FFAA D Ciber EB PEstrt FFAA D Ciber FAB	VII-6	Estudo Interdis- ciplinar de Campo (Brasília)	Feriado N.S. Aparecida Dsloc BSB -12/10	III-7	Exercício de Decisão Estratégica (CIBERPOL)	VII-8	Exc Sml CIBERINFRA	FERIADO FINADOS	
Grc Vul Infra Crítica Grc Vul Infra Crítica Grc Vul Infra Crítica Grc Vul Infra Crítica Grc Vul Infra Crítica			ComDCiber 13/10-M	III-7	Exercício de Decisão Estratégica (CIBERPOL)	VII-8	Exc Sml CIBERINFRA	VII-7	Visita de Estudos ao LaSC do IME
Rede Rio e Rede Hermes Quântica			SERPRO 13/10-T					II-3 II-4	Paradig Geopol Mundial, Ciber e Soberania Nacional – Exercício
Criptologia Criptologia Criptologia Criptologia Criptologia			GSI 14/10-M	III-7	Exercício de Decisão Estratégica (CIBERPOL)	VII-8	Exc Sml CIBERINFRA	II-3 II-4	Paradig Geopol Mundial, Ciber e Soberania Nac – Exercício
Estratégia de dissuasão no espaço cibernético			DPF 14/10-T					II-3 II-4	Paradig Geopol Mundial, Cibere Soberania Nac – Apresent GT
Teo e Ger Cri Ciber Teo e Ger Cri Ciber Teo e Ger Cri Ciber Teo e Ger Cri Ciber Teo e Ger Cri Ciber			ABIN 15/10-M	III-7	Exercício de Decisão Estratégica (CIBERPOL)	VII-8	Exc Sml CIBERINFRA	II-3 II-4	Tec e Anl Psq - Apres Ensaio Acadêmico
Fenom Terror Fenom Terror Fenom Terror			MJSP 15/10-T					Trein Cer Encerramento Mdd Adm Análise Curso -ASPIAvE Mdd Adm Análise Curso -ASPIAvE Mdd Adm Análise Curso -ASPIAvE	
Intlg Estrt Intlg Estrt Intlg Estrt Intlg Estrt Intlg Estrt			MD/CHOC 16/10-M	III-7	Exercício de Decisão Estratégica (CIBERPOL)	VII-8	Exc Sml CIBERINFRA	Medidas Administrativas -DACTEC	
								CERTIFICAÇÃO	
EPI					Dsloc Rio 16/10-T	EPI		EPI	

APÊNDICE AIII

PLANO DE DISCIPLINAS

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - I - POLÍTICA E CIBERESPACO

DISCIPLINA	I - POLÍTICA E CIBERESPAÇO		Cg H Total: 35 h
COMPETÊNCIA PRINCIPAL: Assessorar órgãos governamentais e institucionais nos níveis político e estratégico em assuntos ligados ao ciberespaço.			
UNIDADES DE COMPETÊNCIAS: Estudar os fatores políticos aos quais o Brasil está inserido. Contribuir na elaboração de políticas e estratégias que tratem do ciberespaço.			
ELEMENTOS DE COMPETÊNCIAS: Compreender a atuação dos elementos de Ciência Política. Executar procedimentos na área da cibernética, alinhados com as diretrizes dos Poderes Nacionais.			
CONTEÚDO: ASPECTOS FUNDAMENTAIS DA CONJUNTURA POLÍTICA E CIBERESPAÇO	Cg H:	EIXO TRANSVERSAL	PADRÃO DE DESEMPENHO
ASSUNTOS:			
1. Política e Poder - Teorias do Poder	3	Objetividade Análise Sintetização	Reconhecer o fenômeno do Poder nas relações e estruturas sociais e institucionais.
2. Poder Nacional e Teorias de Estado	3	Atenção seletiva Sintetização	Identificar os fenômenos do Estado, sua estrutura, organização, funcionamento e suas finalidades.
3. Política Contemporânea e Ciberespaço	3	Atenção seletiva Sintetização	Fundamentar o entendimento da atual conjuntura política com base no fenômeno político para apoiar as atividades de planejamentos políticos e estratégicos na dimensão do espaço cibernético.
4. Política, Sociedade e Parceria Público Privada na Dimensão Cibernética.	3	Objetividade Coerência Atenção seletiva Planejamento	Identificar os principais aspectos da conjuntura política, da sociedade e das parcerias público-privada no trato das atividades no espaço cibernético.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - I - POLÍTICA E CIBERESPACO

5. Poder Nacional e Objetivos Nacionais	2	Atenção seletiva Sintetização	Identificar o Poder Nacional como instrumento de que dispõe a Nação para a execução da Estratégia Nacional, com vistas à consecução da Política Nacional.
6. Política Nacional e o Poder Cibernético Nacional	2	Objetividade Coerência Atenção seletiva Planejamento	Caracterizar a Política Nacional como instrumento orientador da aplicação do Poder Cibernético Nacional na busca dos interesses expressos nos Objetivos Nacionais. Identificar os principais aspectos da conjuntura política do Brasil presentes na dinâmica entre poderes da república, a fim de contribuir na formulação de políticas e estratégias do Brasil e institucionais no contexto do poder cibernético.
7. Estratégia Nacional e a Dimensão Cibernética	2	Atenção seletiva Sintetização	Reconhecer os fundamentos axiológicos como elementos definidores de necessidades, interesses e aspirações de uma nação. Identificar o papel dos interesses nacionais como fatores determinantes de objetivos nacionais. Identificar fatores condicionantes do estabelecimento de objetivos nacionais no campo da cibernética. Identificar a ENDC e E-Ciber.
8. Segurança e Defesa Nacionais e a Dimensão Cibernética	2	Atenção seletiva Sintetização	Compreender os conceitos de segurança e de defesa Nacionais e as suas relações com o poder e com o desenvolvimento nacional.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - I - POLÍTICA E CIBERESPACO

09. Expressões do Poder Nacional.	3	Atenção seletiva Sintetização	Compreender a pertinência, a relevância e as inter-relações de ações e de aspectos nos campos das expressões do poder nacional, reconhecendo seus contributos como instrumento de alcance, conquista e preservação de objetivos nacionais.
10. Fenomenologia do Terrorismo	3	Atenção seletiva Sintetização	Compreender as visões sobre questões ligadas ao terrorismo.

CONTEÚDO: ASPECTOS FUNDAMENTAIS DA CIBERPOLÍTICA	Cg H:	EIXO TRANSVERSAL	PADRÃO DE DESEMPENHO
ASSUNTOS:			
11. Fundamentos da Ciberpolítica	4	Objetividade Análise Sintetização	Reconhecer a relação da cibernética com a Política de Estado.
12. Relação entre Ciberpolítica, Geopolítica, Estratégias dos Estados, Marcos Normativos de Cibernética e Relações Internacionais	3	Atenção seletiva Sintetização	Identificar a conexão direta entre as questões digitais e os interesses geopolíticos e estratégicos dos Estados.

AVALIAÇÃO DA APRENDIZAGEM	2		
----------------------------------	---	--	--

ORIENTAÇÕES METODOLÓGICAS
1. Objetivos da Aprendizagem

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - I - POLÍTICA E CIBERESPACO

Assunto 1

- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).
- Identificar a evolução cultural da sociedade como conformadora de valores e princípios nacionais formadores da base axiológica da sociedade brasileira: características essenciais aplicáveis a um processo de planejamento estratégico (FACTUAL).

Assunto 2

- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).
- Identificar a complexidade das relações políticas e os dilemas éticos com os quais os agentes políticos se deparam em seu trabalho (FACTUAL).
- Estabelecer a ponte entre contribuições teóricas e o entendimento cotidiano e profissional da política (CONCEITUAL).

Assuntos 3

- Compreender o estado como instituição política diferenciando-o de nação (CONCEITUAL).
- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).
- Identificar as etapas e aspectos da evolução histórica do Estado (FACTUAL).
- Compreender as tendências da evolução do estado (CONCEITUAL).

Assunto 4

- Identificar os principais aspectos do pensamento político contemporâneo a luz das teorias de Maquiavel, Hobbes, Locke e Rousseau (FACTUAL).
- Analisar as ingerências do espaço cibernético na democracia (CONCEITUAL).
- Discutir as atuais ideologias políticas: o liberalismo, a social-democracia e o socialismo (CONCEITUAL).
- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).

Assunto 5

- Analisar as políticas, as estratégias, os planos, as ações de órgãos setoriais do Governo Brasileiro e as parcerias público privada de interesse estratégico para o setor do espaço cibernético e para a Defesa (CONCEITUAL).
- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).

Assunto 6

- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).
- Compreender o Poder Nacional: conceito, características, estrutura, expressões, potencial e aplicação (CONCEITUAL).

Assunto 7

- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - I - POLÍTICA E CIBERESPACO

- Compreender os conceitos e desdobramentos de Política, da relação entre política e poder, da relação entre política e ética, da Política Nacional, Política de Estado e Política de Governo, considerando a dimensão cibernética (CONCEITUAL).

Assunto 8

- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).
- Reconhecer os conceitos e desdobramentos de Estratégia Nacional, de Estado e de Governo (CONCEITUAL).
- Identificar as inter-relações, ações, trajetórias, e áreas estratégicas envolvendo a Política e a Estratégia, considerando a dimensão cibernética (FACTUAL).

Assunto 9

- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).
- Reconhecer os conceitos de Segurança e Defesa Nacionais, Segurança e Defesa Públicas, os níveis de segurança e as inter-relações entre Desenvolvimento, Segurança e Defesa, considerando a dimensão cibernética (FACTUAL).

Assunto 10

- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).
- Identificar os antecedentes históricos (internacionais e nacionais) dos campos de Expressão do Poder Nacional, os conceitos correlatos, os pré-requisitos, os projetos estratégicos (e ações afetas), os setores e recursos envolvidos (humanos, materiais e financeiros) (FACTUAL).

2. Procedimentos Didáticos

Assunto 1 a 10 - Fornecer aos alunos textos sobre o assunto com questões para serem discutidas em plenário. A aula pode ser conduzida por professor convidado. Um tempo destinado a debate abordando as questões apresentadas.

. Avaliação da Aprendizagem

Será conduzida com uma carga horária de 2 horas, por meio da avaliação formativa podendo ser trabalhos em grupo, produção de *papers* individuais ou debates.

4. Indicações Básicas de Segurança na Atividade

Não é o caso.

REFERÊNCIAS

ACCIOLI, Wilson. **Teoria Geral do Estado**. Rio de Janeiro: ed. Forense, 1985.
ALBUQUERQUE, Roberto C. **Teoria do Desenvolvimento**. Rio de Janeiro. ESG, 1991.
ALBUQUERQUE, Roberto C. LS-302/93. **Teoria do Desenvolvimento**. Rio de Janeiro: ESG, 1993.
AZAMBUJA, D. **Introdução à Ciência Política**, Porto Alegre: ed. Globo, 2008.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - I - POLÍTICA E CIBERESPACO

- BACHELARD, Gaston. **A filosofia do não: filosofia do novo espírito científico**. Tradução Joaquim Jose Moura Ramos. 5. Rio de Janeiro: ed. Presença, 1991.
- _____. **A formação do espírito científico: contribuição para uma psicanálise do conhecimento**. Tradução Estela dos Santos Abreu. 1. ed. 5. reimpr. Rio de Janeiro: ed. Contraponto, 1996.
- BAUMAN, Zygmunt. **Modernidade líquida**. Tradução Plínio Dentzien. Rio de Janeiro: ed. Zahar, 2001.
- _____. **Vida para consumo: a transformação das pessoas em mercadoria**. Trad. Carlos Alberto Medeiros. Rio de Janeiro: ed. Zahar, 2008.
- BERLE, Adolf Augustos. **Power**. New York: ed. Harcourt, Bruce & Word, 1969.
- BONAVIDES, Paulo. **Do estado Liberal ao Estado social**. Belo horizonte: ed. Del Rey, 1993.
- BONAVIDES, Paulo. **Ciência Política**. Rio de Janeiro: ed. FGV, 1976.
- BOBBIO, Norberto. **O futuro da Democracia**, 8a Ed rev. Trad. Marco Aurélio Nogueira. SP: ed. Paz e Terra, 2002.
- BOURDIEU, Pierre. **O Poder Simbólico**. Rio de Janeiro: Bertrand Brasil. Lisboa: ed. Difel, 1989.
- BRASIL, Escola Superior de Guerra. **Fundamentos Axiológicos, Poder Nacional, Objetivo Nacional, Política Nacional, Estratégia Nacional, Desenvolvimento Nacional e Teoria do Poder**. Nota Complementar de Estudo. Rio de Janeiro: ESG, 2015.
- _____. **Fundamentos do Poder Nacional**. Rio de Janeiro: ESG, 2022.
- BRUTON, Henry J. **Princípios da Economia do Desenvolvimento**. Tradução Auriphebo B. Simões. São Paulo: ed. Atlas, 1969.
- BRUZZONE, Andrés. **Ciberpopulismo: política e democracia no mundo digital**. São Paulo: ed. Contexto, 2021.
- BUCHHEIM, Hans. **Política e Poder**. Barcelona: ed. Alfa, 1985.
- CARBONEL, Carlos. **Metafísica del Bien Comum**. Madrid: ed. Rialp, 1998.
- CARVALHO, José Murilo de. **Cidadania no Brasil: o Longo Caminho**. Rio de Janeiro: ed. Civilização Brasileira, 2021.
- CATLIN, G. E. G. **Tratado de Política**. Rio de Janeiro: Labor Editora, 1964.
- CHANG, Ha-Joon. **Chutando a escada: a estratégia do desenvolvimento em perspectiva histórica**. Tradução Luiz Antônio Oliveira de Araújo. São Paulo: ed. UNESP, 2004.
- CLAUSEWITZ, Carl Phillip Gotieb Von. **Da Guerra**. São Paulo: Ed WMF Martins Fontes, 2010.
- CREVELD, Martin Van. **The Transformation of War**. New York: The Free Press, 1999.
- CULKIN, John M. **A schoolman's guide to Marshall McLuhan**. Saturday Review, [S. l.], p. 51-53, 70-. March 18, 1967. Publicado parcialmente em: The Unz Review: An Alternative Media Selection, [S. l.], 2018. Disponível em: <http://www.unz.org/Pub/SaturdayRev-1967mar18-00051>. Acesso em: 01 abr 2021.
- DALLARI, Dalmo de abreu. **Elementos da Teoria Geral do Estado**. São Paulo: ed. Saraiva, 2003.
- ELLUL, Jacques. **O homem e o dinheiro: aprenda a lidar com a origem de todos os males**. Tradução Luiz Galdino. Curitiba: ed. Palavra, 2008.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - I - POLÍTICA E CIBERESPACO

HESSEN, Johan. **Filosofia dos valores**. Trad. Português. Coimbra. Col. Studium Armênio Amado. Várias edições.

_____. **Ética social**. Tradução de Alípio Maia de Castro. São Paulo: ed. Quadrante, 1983.

FRIEDMAN, Milton. **Capitalismo e liberdade**. Tradução Afonso Celso da Cunha Serra. Rio de Janeiro: ed. LTC, 2014.

FIGUEIREDO, D. **A Teoria do Poder**. São Paulo: ed. Revista dos Tribunais, 1992.

FURTADO, Celso. **O mito do desenvolvimento econômico**. São Paulo: ed. Paz e Terra, 1983.

GABRAITH, Kenneth. **Anatomia do Poder**. São Paulo: ed. Pioneira, 1986.

GETTEL, R. **Historia de las Ideas Políticas**. Rio de Janeiro: ed. Labor Editora, 1930.

HABERMAS, Jürgen. **Mudança estrutural da esfera pública: investigações quanto a uma categoria da sociedade burguesa**. Tradução Flávio R. Kothe. Rio de Janeiro: ed. Tempo Brasileiro, 2003.

HOBBS, Thomas. **Leviatã**. Ed. Martin Claret. São Paulo, 2009.

HOBBS, Eric J. **A era das revoluções 1789-1848**. Tradução Maria Tereza Lopes Teixeira. São Paulo: ed. Paz e Terra, 1979.

_____. **A era do capital 1848-1875**. Tradução Luciano Costa Neto. São Paulo: ed. Paz e Terra, 1988.

HUBERMAN, Leo. **História da riqueza do homem**. Tradução Waltensir Dutra. São Paulo: ed. Zahar, 1982.

HUNTINGTON, Samuel. **Choque das Civilizações**. Rio de Janeiro: ed. Objetiva, 1997.

_____. **O Soldado e o Estado**. Rio de Janeiro: ed. BIBLIEx, 1996.

KEEGAN, John. **Uma História da Guerra**. São Paulo: ed. Companhia de Letras, 1995.

KEYNES, John M. **Teoria geral emprego, do juro e da moeda**. Tradução Mario R. da Cruz. São Paulo: ed. Atlas, 1992.

LANDES, David S. **Prometeu desacorrentado**. Tradução Marisa Motta. Rio de Janeiro: ed. Nova Fronteira, 2005.

LEBRUN, Gérald. **O que é o poder?** São Paulo: ed. Brasiliense, 1995.

LIST, Georg Friedrich. **Sistema nacional de economia política**. Tradução Luiz João Baraúna. São Paulo: ed. Nova Cultural, 1988.

LYRA, Rubens Pinto. **Estado e Cidadania: de Maquiavel à Democracia Participativa**. João Pessoa: ed. UFPB, 2006.

LIMONGI, Fernando. **A Democracia no Brasil: presidencialismo, coalizão partidária e processo decisório**. Artigo Científico. Disponível em: <https://www.scielo.br/j/nec/a/BFxz33vLwN9rRnGy6HQMDbz/>. Acesso em 23 jun2022.

MACHIAVELLI, Niccolò. **O Príncipe**. Comentado por Napoleão Bonaparte. Texto integral. Coleção a Obra Prima de Cada autor. Coor Martin Claret. Bauru: ed. Edipro, 2018.

MALTHUS, Thomas R. **Princípios de economia política: ensaio sobre a população**. Tradução Regis de Castro Andrade, Dinah de Abreu Azevedo, Antônio Alves Cury. São Paulo: ed. Nova Cultural, 1996.

MAYNARD, J. K. **Ciência Política**. Rio de Janeiro: ed. FGV, 2020.

McCRAW, Thomas K. **O profeta da inovação: Joseph Schumpeter e a destruição criativa**. Tradução Clóvis Marques. Rio de Janeiro: ed. Record, 2012.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - I - POLÍTICA E CIBERESPACO

- MILL, John S. **Princípios de economia política e tributação**. Tradução Ivan Weisz Kuck. São Paulo: ed. Abril Cultural, 1988.
- MILLER, David. **Perspectivas de justiça social**. Tradução Ana Barradas. In: *Análise social*, Lisboa, v. XXXIII, n. 146-147, p. 323-339, 2º/3º sem. 1998.
- MOSLEY, Michael; LYNCH, John. **Uma história da ciência**. Tradução Ivan Weisz Kuck. São Paulo: ed. Zahar, 2011.
- MYRDAL, Gunnar. **Contra a corrente: ensaios críticos em economia**. Tradução William Jafé. São Paulo: ed. Campus, 1977.
- ENGELS, Friedrich. **A Consciência Revolucionária da História**. Col. Grandes Cientistas sociais. São Paulo: ed. Ática, 1984.
- MENEGHETTI, Antonio. **A Crise das Democracias Contemporâneas**. São Paulo: ed. Onto, 2007.
- NICOLAU, Jairo. **História do Voto no Brasil**. Rio de Janeiro: ed. Zahar, 2004.
- PERROUX, François. **Economia e sociedade**. Tradução Ruy Jungmann. São Paulo: ed. Duas Cidades, 1961.
- _____. François. **Ensaio sobre a filosofia do novo desenvolvimento**. Trad. L. M. Macaista Malheiros. Lisboa: ed. Fund. Calouste Gulbenkian, 2011.
- POLILLO, Raul de. **100 eventos que abalaram o mundo**. São Paulo: ed. Melhoramentos, 1978.
- POULANTZAS, Nicos. **O Estado, o Poder e o Socialismo**. Rio de Janeiro: ed. Graal, 1985.
- PRELOT, M. **A Ciência Política**. S. Paulo: ed. Difusão Europeia do Livro, 1998.
- RICARDO, David. **Princípios de economia política e tributação**. Tradução Paulo Henrique Ribeiro Sandron. São Paulo: ed. Abril Cultural, 1982.
- RUSSEL, B. **O Poder**. Rio de Janeiro: ed. Zahar, 1979.
- SARAMAGO, José de S. **Discurso pronunciado por José Saramago no dia 10 de dezembro de 1998 no banquete do Prémio Nobel**. Lisboa: Fundação José Saramago, 2014. Disponível em: <https://www.josesaramago.org/discurso-pronunciado-por-jose-saramago-no-dia-10-de-dezembro-de-1998-no-banquete-premio-nobel/>. Acesso em 21 nov 2018.
- _____. **Ensaio sobre a cegueira**. Lisboa: Editorial Caminho, 1995.
- SARTORI, G. **A Política**. Brasília: ed. Universidade de Brasília, 1981.
- SCHUMPETER, Joseph A. **Teoria do desenvolvimento econômico**. Tradução Maria Sílvia Rosas. São Paulo: ed. Abril Cultural, 1982.
- SCHWAB, Klaus. **A quarta revolução industrial**. Tradução Daniel Moreira Miranda. São Paulo: ed. Edipro, 2016.
- SEN, Amartya. **Desenvolvimento como liberdade**. Tradução Laura Teixeira Motta. São Paulo: ed. Cia. das Letras, 2010.
- SICSÚ, João; CASTELLAR, Armando (Orgs.). **Sociedade e economia: estratégias de crescimento e desenvolvimento**. Brasília: ed. IPEA, 2009.
- SIMMEL, Georg. **A metrópole e a vida mental**. Tradução Sérgio Marques dos Reis. In: VELHO, Otávio Guilherme de (Org.). *O fenômeno urbano*. Rio de Janeiro: Guanabara, 1987. p. 11-25.
- SMITH, Adam. **A riqueza das nações**. Tradução Getúlio Schanoski Júnior. São Paulo: ed. Madras, 2018.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - I - POLÍTICA E CIBERESPACO

THUROW, Lester. **Cabeça a cabeça**. Tradução Nivaldo Monticelli Júnior. Rio de Janeiro: ed. Rocco, 1993.
VEIGA, José Eli da. **Desenvolvimento sustentável: o desafio do século XXI**. Rio de Janeiro: ed. Garamond, 2010.
WALTZ, Kenneth N. **O Homem, o Estado e a Guerra: Uma Análise Teórica**. São Paulo: ed. WMF Martins Fontes, 2004.
WEFFORT, Francisco. **Os Clássicos da Política**. São Paulo: ed. África, 2008.
VIDIGAL, Armando Amorim Ferreira. **O Brasil Diante dos Desafios Internacionais em Segurança e Defesa**. Rio de Janeiro: ed. CEPEN, 2009.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - II - GEOPOLÍTICA DO CIBERESPAÇO

DISCIPLINA	II – GEOPOLÍTICA DO CIBERESPAÇO			Cg H Total: 26 h
COMPETÊNCIA PRINCIPAL: Assessorar órgãos governamentais e institucionais nos níveis político e estratégico em assuntos ligados ao ciberespaço.				
UNIDADES DE COMPETÊNCIAS: Estudar os fatores geopolíticos e geoestratégicos aos quais o Brasil está inserido. Participar da elaboração de políticas e estratégias que tratem do ciberespaço.				
ELEMENTOS DE COMPETÊNCIAS: Caracterizar os ambientes geopolítico e geoestratégico e a evolução das conjunturas internacional e nacional. Assessorar nos estudos prospectivos, elaborar cenários do campo digital e promover inovações. Considerar os fatores geopolíticos e geoestratégicos quando da participação na formulação de políticas e diretrizes para o ciberespaço.				
CONTEÚDO: ESTUDO GEOPOLÍTICO DE ÁREAS ESTRATÉGICAS	Cg H:	EIXO TRANSVERSAL	PADRÃO DE DESEMPENHO	
ASSUNTOS				
1. Áreas Estratégicas.	3	Análise Comparação Flexibilidade Coerência	Analisar as áreas estratégicas e o panorama geopolítico, sob o enfoque dos aspectos conjunturais das expressões do poder, de acordo com as fontes das referências, para assessorar na elaboração de políticas e estratégias que impactem a dimensão cibernética.	
2. Panorama Geopolítico.	3			

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - II - GEOPOLÍTICA DO CIBERESPAÇO

CONTEÚDO: ESTUDOS GEOPOLÍTICOS APLICADOS AO CIBERESPAÇO	Cg H:	EIXO TRANSVERSAL	PADRÃO DE DESEMPENHO
ASSUNTOS			
3. Paradigmas da Geopolítica Mundial, Ciberespaço e Soberania Nacional.	8	Atenção seletiva Análise Objetividade Proatividade Criatividade	Interpretar a globalização da informação, a partir do espaço comunicacional instantâneo. Identificar o uso do espaço cibernético para ampliar a integração nacional mediante a construção da opinião pública e da ação estatal. Avaliar o impacto do ciberespaço na soberania nacional
4. Conhecimento e Geopolítica do Ciberespaço. Ciberespaço como vetor estratégico da estruturação em rede da sociedade	3		Analisar o espaço cibernético e a internet, sob o enfoque dos aspectos da inteligência estratégica, para assessorar na elaboração de políticas e estratégias.

CONTEÚDO: GEOPOLÍTICA DO SÉCULO XXI E ESPAÇO CIBERNÉTICO	Cg H:	EIXO TRANSVERSAL	PADRÃO DE DESEMPENHO
ASSUNTOS			
5. Panorama Geopolítico Contemporâneo e o Ciberespaço – A formulação de uma Grande Estratégias Nacional na Era da Cibernética e do Lawfare.	5	Atenção seletiva Capacidade linguística Proatividade Cooperação	Analisar a geopolítica contemporânea e o campo cibernético para assessorar na elaboração de políticas e estratégias.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - II - GEOPOLÍTICA DO CIBERESPAÇO

6. Postura geopolítica, ciberespaço e a condição pós-westfaliana	2	Atenção seletiva Análise	Identificar o espaço cibernético no contexto geopolítico virtual de relação do poder regional e mundial.
AVALIAÇÃO DA APRENDIZAGEM	2		

ORIENTAÇÕES METODOLÓGICAS

1. Objetivos da Aprendizagem

Assunto 1

- Compreender as características das áreas estratégicas segundo as Expressões do Poder Nacional (CONCEITUAL).
- Interpretar as influências das áreas estratégicas na formulação das ações da geopolítica (CONCEITUAL).
- Adequar suas ideias com rapidez, em face de novos argumentos (ATITUDINAL).
- Concluir suas exposições estabelecendo um encadeamento lógico com o que foi apresentado (ATITUDINAL).

Assunto 2

- Compreender o panorama geopolítico contemporâneo (CONCEITUAL).
- Comparar e integrar os principais temas geopolíticos no panorama internacional (CONCEITUAL).
- Adequar suas ideias com rapidez, em face de novos argumentos (ATITUDINAL).

Assunto 3

- Compreender as ingerências das atividades da dimensão cibernética no contexto da globalização (CONCEITUAL).

Assunto 4

- Aplicar os princípios da inteligência estratégica (FACTUAL).
- Compreender a importância do conhecimento estratégico (CONCEITUAL).

Assunto 5

- Integrar os principais temas e cenários geopolíticos aos impactos das atividades do espaço cibernético. (CONCEITUAL).

Assunto 6

- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - II - GEOPOLÍTICA DO CIBERESPAÇO

- Compreender a importância da nova geopolítica gerada pelo território cibernético, a teoria de fronteiras terrestres, e as influências para a aplicação do poder e da soberania do Estado de maneira interligada com essa nova dimensão e as ingerências de seus atores e da sociedade (CONCEITUAL).

2. Procedimentos Didáticos

Assunto 1 a 6 - Fornecer aos alunos textos sobre o assunto com questões para serem discutidas em plenário. A aula pode ser conduzida por professor convidado. Um tempo destinado a debate abordando as questões apresentadas.

3. Avaliação da Aprendizagem

Será conduzida com uma carga horária de 2 horas, por meio da avaliação formativa com trabalhos em grupo, produção de papers individuais e debates.

4. Indicações Básicas de Segurança na Atividade

Não é o caso.

REFERÊNCIAS

- BACKHEUSER, Everardo Adolpho. **Curso de Geopolítica Geral e do Brasil**. Rio de Janeiro: ed. Biblioteca do Exército, 1952. 275 p.
- BECKER, Berta K.; EGLER, Claudio A. G. Brasil: **Uma Nova Potência Regional na Economia-Mundo**. Rio de Janeiro: ed. Bertrand Brasil, 2006.
- BOSSO, João Paulo Cavazzani; BRITO, Amanda de; CASTRO, Carolina de; FIGUEIREDO, Dannel Garcia Barbosa de; GIORDANO, Vitória Rangel; GRASSI, Jéssica Maria; MENEZES, Henrique Ribeiro da Rocha Thássia Barbosa de; PAGLIARI, Graciela de Conti; PINTO, Danielle Jacón Ayres; RÊ, Eduardo de. **A Geopolítica das Estratégias em Defesa Cibernética**: ed. Alpheratz, 2021.
- BRASIL. **Constituição da República Federativa do Brasil**. Brasil, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em 23 jun 22.
- _____. **Lei Complementar Nº 97, de 9 de junho de 1999: Dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas**. Brasil, 1988. Disponível em: http://200.20.16.3/moodle/avp/file.php/96/Lei_complementar_97.pdf. Acesso em 23 jun 22.
- _____. **Livro Branco de Defesa Nacional**. Brasil: 2012. Disponível em: <http://www.defesa.gov.br/arquivos/2012/mes07/lbndn.pdf>. Acesso em 23 jun 22.
- _____. **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Brasil, 2020. Disponível em: http://www.defesa.gov.br/arquivos/estado-e-defesa/ENDPND_Optimized.pdf. Acesso em 23 jun 22.
- _____. Ministério da Defesa. Escola Superior de Guerra. **Manual Básico: Volume I - Elementos Fundamentais**. Rio de Janeiro: ESG, 2014. Disponível em: <http://www.esg.br/images/manuais/ManualBasicoI2014.pdf>. Acesso em 23 jun 22.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - II - GEOPOLÍTICA DO CIBERESPAÇO

- _____. **Manual Básico: Volume II - Assuntos Específicos.** Rio de Janeiro: ESG, 2014. Disponível em: <<http://www.esg.br/images/manuais/ManualBasicoII2014.pdf>. Acesso em 22 jun 22.
- CANÇADO TRINDADE, Antônio Augusto. **O Direito Internacional em um Mundo em Transformação.** São Paulo: ed. Renovar, 2002.
- CASTRO, Therezinha de. **Geopolítica: Princípios, Meios e Fins.** Rio de Janeiro: ed. BIBLIEx, 1999.
- FREITAS, Jorge Manuel da Costa. **A Escola Geopolítica Brasileira: Golbery do Couto e Silva, Carlos de Meira Mattos e Therezinha de Castro.** Rio de Janeiro: ed. Biblioteca do Exército, 2004.
- FROMKIN, David. **Paz e guerra no Oriente Médio: a queda do Império Otomano e a criação do Oriente Médio moderno.** Tradução: Teresa Dias Carneiro. Rio de Janeiro: ed. Contraponto, 2008.
- FRIEDE, Roy Reis. **Ciência Política e Teoria do Estado: Teoria Constitucional e Relações Internacionais.** Rio de Janeiro: ed. Biblioteca do Exército, 2015.
- GONÇALES, Selma Lúcia de Moura; PORTELA, Lucas Soares. **A Geopolítica do Espaço Cibernético sul-Americano: in Conformação de Políticas de Segurança e Defesa Cibernética.** Austral: Revista Brasileira de Estratégia e Relações Internacionais, v.7, n.14, Jul./Dez. 2018,| p. 217 217. Austral. Disponível em: <https://seer.ufrgs.br/austral/article/download>. 2018. Acesso em 22 jun 22.
- HUNTINGTON, Samuel P. **O choque de civilizações e a recomposição da ordem mundial.** Tradução de M. H. C. Côrtes. Rio de Janeiro: ed. Biblioteca do Exército, 1998.
- _____. **O Soldado e o Estado: teoria e política das relações entre civis e militares.** Tradução de José Lívio Dantas. Rio de Janeiro: ed. Biblioteca do Exército, 1996.
- JACKSON, Robert; SORENSEN, Georg. **Introdução às Relações Internacionais: Teorias e Abordagens.** Tradução de Bárbara Duarte. Revisão Técnica de Arthur Ituassu. 2. Ed. revisada ampliada. Rio de Janeiro: ed. Zahar: 2013.
- JINPING, Xi. **A Governança da China, Vol 1 e 2.** Rio de Janeiro: ed. Contraponto Editora, 2020.
- JOBIM, Nelson A.; ETCHEGOYEN, Sérgio W.; ALSINA, João Paulo (Orgs). **Segurança Internacional: Perspectivas Brasileiras.** Rio de Janeiro: ed. FGV, 2010.
- KAPLAN, Robert D. **A Vingança da Geografia: a Construção do Mundo Geopolítico a Partir da Perspectiva Geográfica.** Tradução de Cristiana de Assis Serra. Rio de Janeiro: ed. Elsevier: 2013.
- KISSINGER, Henry. **Ordem Mundial.** Tradução: Cláudio Figueiredo. Rio de Janeiro: ed. Objetiva, 2015.
- _____. Sobre a China. Tradução: Cássio de Arantes Leite. Rio de Janeiro: Objetiva, 2011. MAFRA, Roberto Machado de Oliveira. **Geopolítica: Introdução ao Estudo.** São Paulo: ed. Sicurezza, 2006.
- MAGNOLI, Demétrio (Org). **História da Paz.** São Paulo: ed. Contexto, 2008.
- _____. **História das Guerras.** São Paulo: ed. Contexto, 2008.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - II - GEOPOLÍTICA DO CIBERESPAÇO

- MAZIERO, A. C.; AYRES PINTO, D. J. **Poder cibernético e o espaço internacional: uma perspectiva a partir das teorias das relações internacionais**. In: 7º Encontro da Associação Brasileira de Relações Internacionais – Atores e Agendas: interconexões, desafios e oportunidades, Belo Horizonte, 2019.
- MEIRA MATTOS, Carlos de. **Brasil, geopolítica e destino**. Rio de Janeiro: ed. Biblioteca do Exército, 1975.
- _____. **Geopolítica**. Rio de Janeiro: ed. FGV, 2011.
- _____. **Geopolítica e Modernidade: Geopolítica Brasileira**. Rio de Janeiro: ed. Biblioteca do Exército, 2002.
- NAPOLEONI, Loretta. **A Fênix Islamista: o Estado Islâmico e a Reconfiguração do Oriente Médio**. Tradução: Milton Chaves de Almeida.1. Ed. Rio de Janeiro: ed. Bertrand Brasil, 2015.
- PAGLIARI, Graciela de Conti; PINTO, Danielle Jacon Ayres; RÊ, Eduardo de. **A Geopolítica das Estratégias em Defesa Cibernética**. Rio de Janeiro: ed. Alpheratz, 2021.
- PINTO, Danielle Jacon Ayres; PAGLIARI, Graciela de Conti; GRASSI, Jéssica Maria; GIORDANO, Vitória Rangel; BOSSO, João Paulo Cavazzani; BRITO, Amanda de; CASTRO, Carolina de; FIGUEIREDO Danniel Garcia Barbosa de; RÊ, Eduardo de; ROCHA, Henrique Ribeiro da; MENEZES, Thássia Barbosa de. **A Geopolítica das Estratégias em Defesa Cibernética**. Rio de Janeiro: ed. Alpheratz, 2021.
- REZEK, José Francisco. **Direito Internacional Público: Curso Elementar**. Ed. São Paulo: ed. Saraiva, 2011.
- RUFIN, Jean-Christophe. **O Império e os Novos Bárbaros**. Trad. André Amado. Ed. Rio de Janeiro: ed. BIBLIEx, 1996.
- SILVA, Francisco Carlos Teixeira da (Org). **Enciclopédia de Guerras e Revoluções do Século XX**. Rio de Janeiro: ed. Campus, 2004.
- SILVA, Golbery do Couto e. **Geopolítica do Brasil**. Rio de Janeiro: ed. J. Olympio, 1967.
- TOSTA, Octávio. **Teorias Geopolíticas**. Rio de Janeiro: ed. BIBLIEx, 1984.
- TOYNBEE, Arnold. **A Humanidade e a Mãe-Terra: Uma História Narrativa do Mundo**. Trad. Helena Maria Camacho Martins Pereira e Alzira Soares da Rocha. Revisão Técnica de Lincoln de Abreu Penna. Rio de Janeiro: ed. Zahar Editores, 1978.
- TRAVASSOS, Mário. **Projeção Continental do Brasil**. Rio de Janeiro: EME, 1933.
- VESENTINI, José William. **Novas Geopolíticas**. São Paulo: ed. Contexto, 2003.
- VOEGELIN, Eric. **A Nova Ciência da Política**. Trad. José Viegas Filho 2. Brasília: Ed. Editora Universidade de Brasília, 1982.
- WALZER, Michael. **Guerras Justas e Injustas: Uma Argumentação Moral com Exemplos Históricos**. São Paulo: ed. Martins Fontes, 2003.
- WIRTZ, James et Alli. **Strategy in the Contemporary World: Introduction to Strategy Studies**. NY: Oxford University Press, 2002

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - III - ESTRATÉGIA DO CIBERESPAÇO

DISCIPLINA	III - ESTRATÉGIA DO CIBERESPAÇO		Cg H Total: 56 h
COMPETÊNCIA PRINCIPAL: Assessorar órgãos governamentais e institucionais nos níveis político e estratégico em assuntos ligados ao ciberespaço.			
UNIDADE DE COMPETÊNCIA: Assessorar a elaboração de políticas e estratégias que tratem do ciberespaço.			
ELEMENTOS DE COMPETÊNCIAS: Caracterizar os ambientes geopolítico e geoestratégico e a evolução das conjunturas internacional e nacional. Identificar a perspectiva global do ciberespaço. Realizar estudos prospectivos, elaborar cenários do campo digital e promover inovações. Considerar os fatores geopolíticos e geoestratégicos quando da formulação de políticas e diretrizes para o setor cibernético.			
CONTEÚDO: ASPECTOS FUNDAMENTAIS DA CONJUNTURA E CIBERESPAÇO	Cg H:	EIXO TRANSVERSAL	PADRÃO DE DESEMPENHO
ASSUNTOS			
1. Evolução do pensamento estratégico.	3	Análise Objetividade Proatividade	Interpretar os fundamentos da estratégia, considerando a influência da cultura digital, para participar da análise e acompanhamento da conjuntura e da cultura estratégica da dimensão cibernética dos países.
2. Estratégias de segurança nacional e internacionais relacionadas com a dimensão cibernética.	2	Análise Objetividade	
3. Teoria de crise. 3.1 Conceitos e dimensões da crise. 3.2 Gerenciamento de crise. 3.3 Etapas na condução de crise.	8	Atenção seletiva Análise Proatividade Organização	Identificar os níveis de análise de situações de crise para orientar o seu gerenciamento.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - III - ESTRATÉGIA DO CIBERESPACO

4. Espaço cibernético como vetor estratégico da estruturação em rede da sociedade.	2	Análise	Identificar o desenvolvimento social, cultural e econômico desencadeados pelas tecnologias digitais.
5. Atividades cibernéticas e computação quântica.	3	Análise Objetividade Proatividade	Interpretar e identificar os efeitos da computação quântica nas atividades cibernéticas.
6. Casos históricos de ciberataques.	13	Análise Objetividade	Apresentar, a partir das lições aprendidas (<i>cases</i>) e exercícios de simulação, proposições para a ciberproteção, com as ações preventivas e corretivas para sistema financeiro.
7. Políticas e estratégias nacionais e institucionais para a dimensão cibernética, considerando os fatores geopolíticos e geoestratégicos.	21	Planejamento Resolução de problemas Persuasão	Considerar um dos desempenhos abaixo. 1. Utilizando as ferramentas da Metodologia da Pesquisa Científica, apresentar proposições para as políticas e estratégias nacionais e institucionais, considerando a dimensão cibernética, com base nos Marcos Normativos e aplicadas ao tema de segurança e ciberdefesa. 2. Utilizando metodologia de cenários prospectivos e com base na doutrina referente ao espaço cibernético, apresentar propostas para a atualização doutrinária da dimensão cibernética. 3. Exercício de decisão estratégica (CIBERPOL). Apresentar proposições para as políticas e estratégias do Sistema Militar de Defesa Cibernética, para a Doutrina Militar Cibernética relacionadas com ações de ciberdefesa e cibersegurança.
AVALIAÇÃO DA APRENDIZAGEM	2		

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - III - ESTRATÉGIA DO CIBERESPACO

ORIENTAÇÕES METODOLÓGICAS

1. Objetivos da Aprendizagem

Assunto 1 - Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).

- Compreender conceitos básicos de estratégia (CONCEITUAL).
- Compreender o processo de evolução do pensamento estratégico (CONCEITUAL).
- Identificar os níveis, dimensões e extensão da estratégia na era digital (CONCEITUAL).
- Identificar estratégias nacional e militar (CONCEITUAL).

Assunto 2

- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).

- Compreender os fundamentos que caracterizam a cultura estratégica das diferentes nações e como se constitui em condicionante para a formulação de estratégias (CONCEITUAL).

- Caracterizar a cultura estratégica dos países (CONCEITUAL).

- Caracterizar a influência das atividades do espaço cibernético na globalização (CONCEITUAL).

Assunto 3

- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).

- Compreender os fundamentos que tratam da crise: conceito, tipo, atores, objetivo, desafio (CONCEITUAL).

- Compreender os dilemas envolvidos na gestão de uma crise e o propósito de uma manobra de crise (CONCEITUAL).

Assunto 4

- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).

- Identificar as influências do uso das tecnologias digitais nas atividades sociais, culturais e econômicas (CONCEITUAL).

Assunto 5

- Concluir suas exposições estabelecendo um encadeamento lógico com o que foi apresentado (ATITUDINAL).

- Compreender o papel dos meios militares no decorrer de uma crise e aplicação das ferramentas cibernéticas. (CONCEITUAL).

- Analisar a influência de ataques cibernéticos na estratégia nacional (CONCEITUAL).

- Identificar os níveis de condução da manobra de crise cibernética, as dimensões estratégicas e as etapas de desenvolvimento da crise (CONCEITUAL).

Assunto 6

- Concluir suas exposições estabelecendo um encadeamento lógico com o que foi apresentado (ATITUDINAL).

- Examinar um estudo de casos históricos de ataques cibernéticos de crise cibernética nacional e internacionais (CONCEITUAL).

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - III - ESTRATÉGIA DO CIBERESPACO

- Examinar o desenvolvimento da crise cibernética como um estudo de caso (CONCEITUAL).
- Exercício de formulação de proposições estratégicas para cibersegurança do Setor Financeiro Nacional a partir da escolha de um cenário geopolítico mundial, mediante Trabalho.

Assunto 7

- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).
- Reconhecer questões relativas à exploração do espaço cibernético em consonância com os marcos legais (FACTUAL).
- Atuar em Trabalho de Grupo em atividade que exige decisão estratégica (CIBERPOL).
- Expressar, com facilidade (ou naturalidade), suas opiniões ou questionamentos (ATITUDINAL).
- Ser convincente em suas atitudes e palavras (ATITUDINAL).
- Exercício para formulação de proposições para as políticas e estratégias nacionais e institucionais para a dimensão cibernética, considerando os fatores geopolíticos e geoestratégicos, mediante Trabalho.

2. Orientações para Execução de Situação-Problema

Para o exercício de crise, os alunos deverão ser organizados em grupos, com grupos atuadores e grupo contestador. Deverá ser apresentado um cenário de crise cibernética nacional ou internacional em futuro próximo e solicitado aos grupos atuadores propostas de medidas para a gestão da crise, seguindo-se de painéis avaliadores, nos quais o grupo contestador deverá apresentar as dificuldades naturais de implementação daquelas propostas.

3. Procedimentos Didáticos

Assunto 1 a 6 - Repassar aos alunos as fontes de consulta e os artigos de preparação para a aula com questões para serem discutidas em plenário. Conduzir a aula com palestra e discussão dirigida. A aula pode ser conduzida por professor convidado.

Assunto 7 - Aplicar os conceitos no exercício de crise com abordagem em cenário prospectivo.

4. Avaliação da Aprendizagem

Será conduzida com uma carga horária de 2 horas, por meio da avaliação formativa em grupo, com a execução do exercício de crise.

5. Indicações Básicas de Segurança na Atividade

Não é o caso.

REFERÊNCIAS

ARON, Raymond. **Paz e Guerra Entre as Nações**. São Paulo: Imprensa Oficial do Estado, 2002.
_____. **Pensar a Guerra**, Clausewitz. 2V Brasília: ed. UnB, 1986.
BEAUFRE, André. **Introdução à Estratégia**. Rio de Janeiro: ed. BIBLIEx, 1998.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - III - ESTRATÉGIA DO CIBERESPACO

BOBBITT, Philipe. **A Paz e a Guerra na História Moderna**. Rio de Janeiro: ed. Campus, 2003.

CLAUSEWITZ, Carl Von. **Da Guerra**. São Paulo: ed. Martins Fontes, 1979.

CREVELD, Martin Van. **The Transformation of War**. New York: The Free Press, 1999.

COUTEAU-BEGARIE, Hervé. **Tratado de Estratégia**. Rio de Janeiro: versão autorizada ao Sv Doc Marinha, 2006.

GRAY, Colin S. **Modern Strategy**. New York: Oxford University Press, 1991.

FULLER, J. F. C. **A Conduta da Guerra**. Rio de Janeiro: ed. BIBLIEx, 2002.

KEEGAN, John. **Uma História da Guerra**. São Paulo: ed. Companhia de Letras, 1995.

KISSINGER, Henry. **Ordem Mundial**. Rio de Janeiro: ed. Objetiva, 2014.

LIDDELL HART, B. H. **As Grandes Guerras da História**. São Paulo: ed. Ibrasa. 1982.

MAGALHÃES; Marcus Abreu; SYDOW, Spencer Toth. **Cyberterrorismo: a nova era da criminalidade**. Belo Horizonte: ed. D'Plácido. 2018.

MEIRA MATTOS, Carlos. **Estratégias Militares Dominantes**. Rio de Janeiro: ed. BIBLIEX, 1986.

MORGENTHAU, Hans. **Política Entre as Nações: A Luta Pelo Poder e Pela Paz**. São Paulo: ed. Martins Fontes, 2004.

PARET, Peter. **Construtores da Estratégia Moderna: de Maquiavel à Era Nuclear**. Rio de Janeiro: ed. BIBLIEX, 2016.

BIBLIEx. RAWLS, John. **O Direito dos Povos**. São Paulo: ed. Martins Fontes, 2002.

WALTZ, Kenneth N. **O Homem, o Estado e a Guerra: Uma Análise Teórica**. São Paulo: ed. Martins fontes, 2004.

WALZER, Michael. **Guerras Justas e Injustas: Uma Argumentação Moral com Exemplos Históricos**. São Paulo: Martins Fontes, 2003.

WIRTZ, James et Alli. **Strategy in the Contemporary World: Introduction to Strategy Studies**. Nova Iorque: ed. Oxford University Press, 2002.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - IV - RELAÇÕES INTERNACIONAIS E CIBERESPAÇO

DISCIPLINA	IV - RELAÇÕES INTERNACIONAIS E CIBERESPAÇO			Cg H Total: 20 h
COMPETÊNCIA PRINCIPAL: Assessorar órgãos governamentais e institucionais nos níveis político e estratégico em assuntos ligados às Relações Internacionais e o Ciberespaço.				
UNIDADES DE COMPETÊNCIAS: Estudar os fatores geopolíticos e geoestratégicos aos quais o Brasil está inserido. Realizar estudos, planejamentos e proposições, no nível político-estratégico, considerando os conceitos e fundamentos das Relações Internacionais.				
ELEMENTO DE COMPETÊNCIA: Conhecer as Relações Internacionais, a ciberdiplomacia praticada pelo Brasil e as parceiras estratégicas. Assessorar no estudo da influência dos conflitos cibernéticos nas Relações Internacionais e na soberania do Estado.				
CONTEÚDO: ASPECTOS FUNDAMENTAIS DAS RELAÇÕES INTERNACIONAIS E CIBERESPAÇO	Cg H:	EIXO TRANSVERSAL	PADRÃO DE DESEMPENHO	
ASSUNTOS				
1. Teoria das Relações Internacionais e Ciberespaço.	4	Análise Objetividade Coerência	Identificar as teorias que orientam as relações entre os Estados Nacionais, baseando-se nas fontes das referências e literatura existente, para realizar a análise e o acompanhamento da conjuntura internacional e nacional	
2. Fundamentos do Direito Internacional e Direitos Humanos no Ciberespaço.	4		Interpretar as injunções do Direito Internacional na regulação dos relacionamentos interestatais, tendo por base os estudos e jurisprudências existentes, para realizar a análise e o acompanhamento da conjuntura internacional e nacional.	

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - IV - RELAÇÕES INTERNACIONAIS E CIBERESPAÇO

3. Ciberdiplomacia.	2	Análise Objetividade	Identificar o impacto das tecnologias digitais na diplomacia moderna. Identificar a dinâmica da segurança e defesa cibernéticas nas relações internacionais. Identificar a condução da diplomacia na era digital.
4. Impactos das atividades cibernéticas na agenda de paz e segurança.	2	Análise Objetividade	Identificar o impacto das tecnologias digitais na agenda de paz e segurança.
5. Posicionamentos e iniciativas diplomáticas dos diversos países no cenário internacional na dimensão do Ciberespaço 5.1 Posicionamento da ONU: Assembleia Geral, GGEs e OEWGs. 5.2 Posicionamento diplomático dos EUA quanto ao Ciberespaço. 5.3 Posicionamento diplomático do Reino Unido quanto ao Ciberespaço. 5.4 Posicionamento diplomático da França quanto ao Ciberespaço. 5.5 Posicionamento diplomático da Holanda quanto ao Ciberespaço. 5.6 Posicionamento diplomático da China quanto ao Ciberespaço. 5.7 Posicionamento diplomático da Rússia quanto ao Ciberespaço. 5.8 Posicionamentos político, estratégico e diplomático no âmbito do Ciberespaço do Brasil no cenário internacional.	6	Análise Objetividade Coerência	Interpretar os principais temas que regem as relações entre os estados, baseando na literatura existente e nas ocorrências da atualidade no campo da cibernética, para realizar a análise e o acompanhamento da conjuntura internacional e nacional.
AVALIAÇÃO DA APRENDIZAGEM	2		

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - IV - RELAÇÕES INTERNACIONAIS E CIBERESPAÇO

ORIENTAÇÕES METODOLÓGICAS

1. Objetivos da Aprendizagem

Assunto 1

- Descrever as principais teorias das relações internacionais (FACTUAL).
- Compreender o posicionamento do Brasil ante os organismos internacionais (CONCEITUAL).

Assunto 2

- Discutir os fundamentos do direito internacional (CONCEITUAL).
- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).
- Mostrar-se participativo e solícito nas atividades de seu grupo (ATITUDINAL).

Assunto 3

- Compreender os dispositivos legais e os tratados e convenções do direito internacional no campo da cibernética e suas implicações no relacionamento do Brasil com outras Nações, (CONCEITUAL).
- Compreender a dinâmica brasileira no contexto da ciberdiplomacia (FACTUAL).
- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).
- Mostrar-se participativo e solícito nas atividades de seu grupo (ATITUDINAL).

Assunto 4

- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).
- Compreender a interferência da dimensão cibernética na agenda de paz e segurança (FACTUAL).

Assunto 5

- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).
- Compreender a dinâmica internacional no contexto da ciberdiplomacia (FACTUAL).

2. Procedimentos Didáticos

Assunto 1 a 5 - Fornecer aos alunos textos sobre o assunto com questões para serem discutidas em plenário. A aula pode ser conduzida por professor convidado. Um tempo destinado a debate abordando as questões apresentadas.

3. Avaliação da Aprendizagem

- Será conduzida com uma carga horária de 2 horas, por meio da avaliação formativa com trabalhos em grupo, produção de papers individuais e debates.

4. Indicações Básicas de Segurança na Instrução

- Não é o caso.

REFERÊNCIAS

ALMEIDA, Virgílio. FILGUEIRAS, Fernando. **Governance for the digital world: Neither more state nor more marketing**. Londres: ed. Palgrave MacMillan, 2020.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - IV - RELAÇÕES INTERNACIONAIS E CIBERESPAÇO

- ALMEIDA, Paulo, Roberto de. **Relações Internacionais e Política Externa Brasileira**. Porto Alegre: ed. da Universidade /UFRGS, 1998.
- ARON, Raymond. **O Estado e as Relações Internacionais**. Brasília: ed. Universidade de Brasília, 1982.
- _____. **Paz e Guerra entre as Nações**. São Paulo: Imprensa Oficial do Estado, 2002.
- BARRINHA, A. & RENARD, T. **Cyber-Dipomacy: The Making of na Intrentional Society in the Digital Age**. Global Affairs, 3:4-5, 353-363. 2017. Disponível em: 10.1080/23340460.2017.1414924. Acesso em: 10 jun 2022.
- BJLO, C., CASSID, J. & MANOR, I. **Public Dipolomacy in the Digital Age**. *The Hague Journal of Diplomacy*, 14(1-2),83-101. 2019. Disponível em: <https://doi.org/10.1163/1871191X-14011032>. Acesso em: 10 jun 2022.
- BOBBITT, Philipe. **A Paz e a Guerra na História Moderna**. Rio de Janeiro: Campus, 2003.
- BOSSO, João Paulo Cavazzani; BRITO, Amanda de; CASTRO, Carolina de; FIGUEIREDO, Danniell Garcia Barbosa de; GIORDANO, Vitória Rangel; GRASSI, Jéssica Maria; MENEZES, Henrique Ribeiro da Rocha Thássia Barbosa de; PAGLIARI, Graciela de Conti; PINTO, Danielle Jacón Ayres; RÊ, Eduardo de. **A Geopolítica das Estratégias em Defesa Cibernética**. Rio de Janeiro: ed. Alpheratz, 2021.
- CARR, Eduard Hallett. **Vinte anos de Crise: 1919-1939. Uma Introdução ao Estudo das Relações Internacionais**. Brasília: ed. Universddidade de Brasília, 2001.
- COMITÊ INTERNACIONAL DA CRUZ VERMELHA. **Convenções de Genebra de 12 de agosto de 1949**. Genebra: CICV, 1992.
- DEUTSCH, K. **A Natureza das Relações Internacionais**. Brasília: ed. Universidade de Brasília, 1982.
- FINNEMORE, M. & HOLLSIS, D. B. **Constructing Norms for /global Cybersecurity**. 110 /*American Journal of International Law*. 2016. Disponível em: <https://www.iilj.org/wp-content/uploads/2017/01/Finnemore-Hollis-Constructing-Norms-for-Global-Cybersecurity.pdf>. Acesso em: 10 jun 2022.
- _____. **Nanub and Shaming: Accusations and International Law in Cibersecurity**. *European Journal of International Law* (forthcoming 2020. Temple University Legal Studies Research Paper nº 2019-14. Disponível em: <https://ssrn.com/abstract=3347958> ou <https://dx.doi.org/10.319/ssrn.3347958>. Acesso em: 10 jun 2022.
- GONÇALVES, Williams. **Relações Internacionais: Um balanço teórico-histórico**. In: TEIXEIRA da Silva, Francisco Carlos (Org). *O Século Sombrio – Uma História Geral do Século XX*. Rio de Janeiro, Campus, 2004, pp. 27-45.
- GUEDES DE OLIVEIRA, Marcos Aurélio; GAMA NETO, Ricardo Borges; LOPES, Gills Vilar (Orgs.). **Relações Internacionais Cibernéticas**. *Revista de Estudos Internacionais (REI)*, ISSN 2236-4811, Vol. 9 (1), 2018. Recife: ed. UFPE, 2016. Disponível em: <www.revistadeestudosinternacionais.com>. Acesso em: 10 jun 2022.
- HICKING, B. & MELISSEN, J. **Dipolomacy in the Digital Age**. *Netherlands Institute of International Relations Clingendael*. Disponível em: https://www.clingendael.org/sites/default/files/pdfs/Digital_Diplomacy_in_the_Digital%20Age_Clingendael_July2015.pdf. Acesso em: 10 jun 2022.
- HOLSTI, Ole R. **Theories of International Relations and Foreign Policy: Realism and Its Challengers**. In: KEGLEY JR., Charles W. *Controversies in International Relations Theory - Realism and the Neoliberal Challenge*. New York, St Martin's Press, 1995, pp. 35-67.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - IV - RELAÇÕES INTERNACIONAIS E CIBERESPAÇO

KURBALIJA, J. Introduction to Internet Governance. Diplo Foundation. 2016. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=UgAtDwAAQBAJ&oi=fnd&pg=PA1&dq=KURBALIJA,+J.+Introduction+to+Internet+Governance&ots=eFH4n8ZdBm&sig=kEK4BAR0LPMpXJM4W1sCH6WuIbs#v=onepage&q=KURBALIJA%2C%20J.%20Introduction%20to%20Internet%20Governance&f=false>. Acesso em: 10 jun 2022.

LÉVY, Pierre. **Cibercultura**. São Paulo: ed. 34. 2010.

LUCERO, Everton. **Governança da Internet: aspectos da Formação de um Regime Global de Oportunidades para a Ação Diplomática**. Fundação Alexandre de Gusmão. Brasília. 2011. Disponível em: http://funag.gov.br/loja/download/822-Governanca_da_Internet.pdf. Acesso em: 10 jun 2022

MAYER-Schönberger, V. & CUKIER, K. **Big Data: A Revolution That Will Transform How We Live, Work, and Think**. Boston: ed. DOLAN/Houghton Mifflin Harcourt. 2014.

MORGENTHAU, Hans. **A Política entre as nações: A Luta pelo Poder e pela Paz**. São Paulo: ed. Imprensa Oficial do Estado de São Paulo, 2003.

NAÇÕES UNIDAS. **Carta das Nações Unidas e Estatuto da Corte Internacional de Justiça**. New York: Serviço de Informação Pública da ONU, 1991.

NOGUEIRA, João Pontes; MESSARI, Nizar. **Teoria das Relações Internacionais: Correntes e Debates**. Rio de Janeiro: ed. Elivier, 2005.

SILVA, Guilherme. **Dicionário de Relações Internacionais**. São Paulo: ed. Manole, 2005.

VILLANOVA, Carlos Luís Duarte. **Diplomacia Pública e Imagem do Brasil no Século XXI**. Brasília: ed. Fundação Alexandre de Gusmão, 2017.

WALTZ, Kenneth N. **Teoria das Relações Internacionais**. Lisboa: ed. Gradiva, 2002.

_____. **O Homem, o Estado e a Guerra: Uma Análise Teórica**. São Paulo: ed. Martins Fontes, 2004.

WIGHT, Martin. **A Política do Poder**. São Paulo: ed. Imprensa Oficial do Estado de São Paulo, 2002.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - V - MARCOS NORMATIVOS E CIBERESPACO

DISCIPLINA	V - MARCOS NORMATIVOS E CIBERESPACO	Cg H Total: 40 h
COMPETÊNCIA PRINCIPAL: Gestar as ciberatividades com respaldo legal.		
UNIDADES DE COMPETÊNCIAS: Assessorar nos estudos e planejamentos de emprego de ações no campo da cibernética e atuar respeitando os marcos normativos nacional e internacional em vigor, referentes à dimensão cibernética. Assessorar nos estudos e proposições nos níveis político e estratégico para o setor de Defesa Nacional e em prol da Segurança Nacional.		
ELEMENTOS DE COMPETÊNCIAS: Interpretar os marcos normativos nacionais em vigor correlacionados à dimensão cibernética. Estudar as legislações internacionais que versam sobre cibernética. Contribuir na investigação de crimes digitais e na realização de perícias forenses, considerando as definições dos cibercrimes e os ilícitos penais praticados com recursos de meios tecnológicos. Participar de estudos para proposições relacionadas com as políticas e estratégias nacionais. Participar da elaboração de proposições para as políticas e estratégias do Sistema Militar de Defesa Cibernética, para a Doutrina Militar Cibernética, com vistas à legalização das ações de segurança e defesa de ciberataques. Caracterizar o cibercrime e os problemas dos países em sua abordagem.		

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - V - MARCOS NORMATIVOS E CIBERESPACO

CONTEÚDO: MARCOS NORMATIVOS APLICADOS AO CIBERESPACO	Cg H:	EIXO TRANSVERSAL	PADRÃO DE DESEMPENHO
ASSUNTOS			
1. Marcos Normativos Internacionais e Nacionais Aplicados à Política, à Estratégia e à Defesa considerando o Ciberespaço. EXEMPLOS 1.1 Convenção de Budapeste sobre o Cibercrime. 1.2 Tallinn Manual 2.0 <i>on the International Law Applicable to Cyber Operations</i>. 1.3 Marco de Ação de Hyogo. 1.4 Marco de Sendai. 1.5 Direito Internacional dos Conflitos Armados. 1.6 Direito Digital Internacional - Regulamento da União Europeia (GDPR), 2016/679 do Parlamento Europeu e do Conselho. 1.7 Legislação sobre uso do ciberespaço de outros países. 1.8 Principais políticas cibernéticas (<i>cyber policies</i>)¹. 1.9 Lei nº 11.631, de 27 de dezembro de 2007 – SINAMOB. 1.10 Lei nº 12.527, de 18 de novembro de 2011, Lei de Acesso a informações. 1.11 Lei nº 12.735, de 30 de novembro de 2012, tipifica crimes eletrônicos e digitais. 1.12 Lei nº 12.737, de 30 de novembro de 2012, tipifica delitos informáticos. 1.13 Lei nº 12.965, de 23 de abril de 2014 - Marco Civil da Internet.	27	Compreensão leitora Análise Sintetização Objetividade Coerência	Interpretar os aspectos fundamentais da legislação nacional e internacional, de acordo com as fontes das referências, para realizar a análise e a inter-relação com as atividades no campo da cibernética.

¹ *Policy Paper* – Documento expedido por um Estado, a fim de explicitar/comunicar perante a comunidade internacional as considerações/normas que aquele país observa, no trato de temas específicos, como a cibernética; entre os mais comuns estão os *white papers*, como o Livro Branco de Defesa Nacional.

ESCOLA SUPERIOR DE GUERRA

CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - V - MARCOS NORMATIVOS E CIBERESPACO

1.14 Lei nº 13.260, de 16 de março de 2016. 1.15 Lei nº 13.675, de 11 de junho de 2018, organização da segurança pública. 1.16 Lei nº 13.709, de 14 de agosto de 2018 alterada pela Lei nº 13.853, de 8 de julho de 2019 - Lei Geral de Proteção de Dados Pessoais. 1.17 Lei nº 13.844, de 18 de junho de 2019. 1.18 Lei nº 14.155, de 27 de maio de 2021, amplia penas para crimes cibernéticos. 1.19 Livro Branco de Defesa Nacional. 1.20 Política Nacional de Defesa. 1.21 Política Nacional de Segurança de Infraestruturas Críticas. 1.22 Política Nacional de Defesa Cibernética. 1.23 Política Nacional de Segurança da Informação. 1.24 Estratégia Nacional de Segurança Cibernética (E-CIBER). 1.25 Estratégia Nacional de Segurança da Informação. 1.26 Estratégia Nacional de Defesa. 1.27 Estratégia Nacional de Defesa Cibernética. 1.28 Estratégia Nacional de Segurança de Infraestruturas Críticas. 1.29 Diretrizes de Segurança Cibernética para os Setores Nacionais. 1.30 Diretrizes de Defesa Cibernética para os Setores Nacionais. 1.31 Regulamentação da Tecnologia da Informação da Secretaria de Governo Digital –Ministério da Economia. 1.32 Decreto nº 10.748, de 19 de julho de 2021, Rede Federal de Gestão de Incidentes Cibernéticos (REGIC). 1.33 Decreto nº 10.332, de 28 de abril de 2020, Estratégia de Governo Digital			
--	--	--	--

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - V - MARCOS NORMATIVOS E CIBERESPACO

1.34 Decreto nº 11.856, de 26 de dezembro de 2023, Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança.			
1.35 Portaria Normativa nº 297/EMCFA/MD, de 5 de fevereiro de 2015 que aprova o Manual de Mobilização Militar – MD41-M-02.			
1.36 Portaria Normativa nº 2.330/MD, de 28 de outubro de 2015. Aprova a "Doutrina de Mobilização Militar- MD41-M-01 (2a Edição/2015).			
1.37 Outros documentos normativos editados no ano em questão			
2. Cibercrimes e Legislação Penal.	2		
3. Marcos Normativos de Gestão Forense Aplicável ao Ciberespaço - Obtenção e Aplicação Judiciária de Evidências Forenses Cibernéticas.	2	Análise Raciocínio dedutivo Cooperação Objetividade Proatividade	Identificar os problemas nacionais e internacionais na caracterização de crime cibernético. Interpretar os aspectos fundamentais da computação forense e identificar os crimes virtuais, para realizar a análise e a inter-relação com as atividades no campo da cibernética.
4. Normas para Preservação de Evidências em Crimes Digitais.	2		
5. Marcos Normativos do Ministério da Defesa Aplicável ao Ciberespaço. 5.1 Fundamentos de Segurança e Defesa do Ciberespaço no Âmbito da Defesa. 5.2 Política Cibernética de Defesa (MD31-P-02). 5.3 Sistema Militar de Defesa Cibernética (SMDC). 5.4 Doutrina Militar de Defesa Cibernética.	5	Análise Raciocínio dedutivo Objetividade Proatividade	Interpretar os aspectos fundamentais da legislação do Ministério da Defesa e das FFAA, de acordo com as fontes das referências, para realizar a análise e a inter-relação com as atividades no campo da cibernética.

ESCOLA SUPERIOR DE GUERRA

CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - V - MARCOS NORMATIVOS E CIBERESPACO

5.5 Legislação do Ministério da Defesa e das FFAA Referentes ao Ciberespaço. 5.6 Fundamentação para Legalização das Ações de Segurança e Defesa de Ciberataques. 5.7 Código Penal Militar - Cibercrimes e Legislação Penal Militar. 5.8 Portaria GM-MD nº 4174, de 16 de agosto de 2023, Aprova o Plano Setorial de Gestão de Incidentes Cibernéticos do Setor Defesa (PSGIC-Def).			
AVALIAÇÃO DA APRENDIZAGEM	2		

ORIENTAÇÕES METODOLÓGICAS

1. Objetivos da Aprendizagem

Assunto 1

- Identificar a complexidade dos marcos normativos, o espaço cibernético e os dilemas éticos dos agentes políticos e das instituições (FACTUAL)

- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).

- Reconhecer questões relativas à dimensão cibernética e como atuar com legalidade (FACTUAL)

- Estabelecer a ponte entre contribuições teóricas e o entendimento cotidiano e profissional do uso do espaço cibernético (CONCEITUAL)

Assuntos 2

- Compreender a utilização do ciberespaço no âmbito social, conflitos e jurídico (CONCEITUAL).

- Identificar os crimes virtuais, bem como as possíveis consequências jurídicas aplicadas atualmente na legislação vigente (CONCEITUAL).

- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).

- Identificar os aspectos jurídicos relacionados com o ciberespaço (FACTUAL).

- Compreender as tendências da evolução do uso do ciberespaço e sua implicação jurídica (CONCEITUAL).

Assunto 3

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - V - MARCOS NORMATIVOS E CIBERESPACO

- Compreender os conceitos fundamentais da gestão forense e seus impactos no uso do ciberespaço (CONCEITUAL).
 - Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).
- Assunto 4
- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).
 - Identificar fundamentos jurídicos que orientam os procedimentos para preservar as evidências de crimes digitais (FACTUAL).
- Assunto 5
- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).
 - Conhecer os conceitos fundamentais das normatizações da Defesa referentes ao uso do ciberespaço (CONCEITUAL).

2. Procedimentos Didáticos

Assunto 1 a 5 - Fornecer aos alunos textos sobre o assunto com questões para serem discutidas em plenário. A aula pode ser conduzida por professor convidado. Destinar tempo para condução de debates abordando os aspectos das principais normatizações.

3. Avaliação da Aprendizagem

Será conduzida com uma carga horária de 2 horas, por meio da avaliação formativa com trabalhos em grupo, produção de papers individuais e debates.

4. Indicações Básicas de Segurança na Atividade

Não é o caso.

REFERÊNCIAS

- ASCENSÃO, José de Oliveira. **Direito da internet e da sociedade da informação**. São Paulo: ed. Forense. 2002.
- ATHENIENSE, Alexandre. **A Jurisdição no Ciberespaço**. Disponível em: < <https://core.ac.uk/download/pdf/211925976.pdf>. Acesso em 22 jun 22.
- BIBLIOTECA NACIONAL. Governança em privacidade e proteção de dados: uma visão integrada aos negócios empresariais, livro digital, acesso EM 27/03/23 <https://campanhas.serpro.gov.br/livro-digital-governanca-em-privacidade/>
- BRASIL. **CARTA DAS NAÇÕES UNIDAS**, Decreto nº 19.841. Brasil. 1945.
- _____. **Doutrina Militar de Defesa Cibernética**. Brasil. 2014
- _____. **Doutrina de Operações Conjuntas**. Brasil. 2020
- _____. **Estratégia Nacional de Defesa**. Brasil. 2012.
- _____. **Estratégia Nacional de Segurança Cibernética**. Decreto nº 10.222. Brasil. 2020.
- _____. **Estratégia Nacional de Segurança da Informação**. Brasil. 2019.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - V - MARCOS NORMATIVOS E CIBERESPACO

- _____. **Estratégia Nacional de Segurança de Infraestruturas Críticas.** Decreto nº 10.569, de 9 de dezembro de 2020.
- _____. **Manual de Doutrina Glossário das Forças Armadas, Glossário de Defesa Cibernética.** Brasil. 2015.
- _____. **Manual de Doutrina de Operações Conjuntas, MD30-M-01.** Brasil. 2020.
- _____. **Manual de Operações Interagências, MD-33-M-12,** Brasil. 2017.
- _____. **Lei nº 12.735, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares.** Brasil, 2012.
- _____. **Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal.** Brasil, 2012.
- _____. **Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Brasil, 2014.
- _____. **Lei nº 13.675, de 11 de junho de 2018. Disciplina a organização e o funcionamento dos órgãos responsáveis pela segurança pública, nos termos do § 7º do art. 144 da Constituição Federal; cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS); institui o Sistema Único de Segurança Pública (Susp); altera a Lei Complementar nº 79, de 7 de janeiro de 1994, a Lei nº 10.201, de 14 de fevereiro de 2001, e a Lei nº 11.530, de 24 de outubro de 2007; e revoga dispositivos da Lei nº 12.681, de 4 de julho de 2012.** Brasil, 2018.
- _____. **Lei nº 13.709/18, de 14 de agosto de 2018. Alterada pela Lei nº 13.853, de 18 de julho de 2019, Lei Geral de Proteção de Dados Pessoais.** Brasil, 2018.
- _____. **Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato.** Brasil, 2021.
- _____. **Decreto-Lei nº 6.227, de 24 de janeiro de 1944. Institui o Código Penal Militar.** Brasil, 1944.
- _____. **Decreto nº 849, de 25 de junho de 1993. Promulga os Protocolos I e II de 1977 adicionais às Convenções de Genebra de 1949, adotados em 10 de junho de 1977 pela Conferência Diplomática sobre a Reafirmação e o Desenvolvimento do Direito Internacional Humanitário aplicável aos Conflitos Armados e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança.** Brasil, 2020.
- _____. **Decreto nº 10.474, de 26 de agosto de 2020. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão**
- _____. **Livro Branco de Defesa Nacional.** Brasil. 2012.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - V - MARCOS NORMATIVOS E CIBERESPACO

_____. **Livro Verde Segurança Cibernética no Brasil.** Brasil. 2010.

_____. **Manual de Emprego do Direito Internacional dos Conflitos Armados (DICA) nas Forças Armadas. MD34-M-03.** Ministério da Defesa, 1ª Edição/2011.

_____. **Política Cibernética de Defesa.** Brasil. 2012.

_____. **Política Nacional de Defesa.** Brasil. 2012.

COMITÊ EUROPEU PARA OS PROBLEMAS CRIMINAIS. **Convenção de Budapeste** - sobre o cibercrime. Budapeste, 2001. Disponível em <https://rm.coe.int/16802fa428>. Acesso em 22 jun 22.

MARCO DE AÇÃO DE HYOGO. Disponível em: https://www.defesacivil.pr.gov.br/sites/defesa-civil/arquivos_restritos/files/documento/2018-12/MarcodeHyogoPortugues20052015.pdf. Acesso em 22 jun 22.

MARCO DE SENDAI PARA A REDUÇÃO DO RISCO DE DESASTRES 2015-2030. Disponível em: <https://www.defesacivil.pr.gov.br/Pagina/Legislacao-internacional>. Acesso em 22 jun 22.

TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS. NATO Cooperative Cyber Defence Centre of Excellence. Cambridge University Press. 2013.

UNITED STATES DEPARTMENT OF HOMELAND SECURITY (DHS). **Presidential Policy Directive 21 (PPD-21) Implementation:** An Interagency Security Committee. Washington. 2015.

KUNRATH, Josefa Cristina Tomaz Martins. **A expansão da criminalidade no cyberespaço.** Feira de Santana: Universidade Estadual de Feira de Santana, 2017. Disponível em: <<https://www.uefs.br> > documentos > get_file. Acesso em 22 jun 22.

LÓSSIO, Claudio Joel Brito. **O Direito e o Ciberespaço.** Salvador: ed. Juspodivm, 2022.

ZENI, Paulo César. **Fundamentos do Processo Judicial Eletrônico - E a Defesa dos Direitos no Ciberespaço.** Belo Horizonte: ed. Fórum, 2019.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA
ÉTICA – PLADIS - VI - SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS

DISCIPLINA	VI - SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS	Cg H Total: 49 h
-------------------	---	-------------------------

COMPETÊNCIA PRINCIPAL:

Assessorar no planejamento nos níveis político e estratégico, no contexto de Segurança da Informação e de Proteção de Dados.

UNIDADES DE COMPETÊNCIAS:

Assessorar nos estudos/planejamentos e realizar proposições no âmbito da Segurança da Informação.

Assessorar na análise de planejamentos e proposições, no contexto da LGPD.

Participar de estudos, análises, planejamentos e proposições, nos níveis político e estratégico, considerando as influências das redes sociais e das mídias sociais no âmbito da Segurança da Informação.

Participar de estudos, análises, planejamentos e proposições, nos níveis político e estratégico, no âmbito da segurança e ciberdefesa, identificando as formas de atores adversos no ciberespaço.

ELEMENTOS DE COMPETÊNCIAS:

Apresentar proposições fundamentadas na ética, nas vulnerabilidades, nas formas de atuação e nas medidas de segurança e ciberdefesa, considerando os possíveis ciberataques e segurança da internet, na internet das coisas, na segurança de redes, na segurança dos dispositivos móveis e nas mídias sociais.

Identificar as características das tecnologias em utilização pela internet.

Identificar vulnerabilidades no uso de mídias sociais e dos dispositivos móveis.

Identificar os potenciais problemas estruturais institucionais no âmbito da Segurança da Informação, considerando o sistema de produção, de gestão, de monitoramento e de tratamento de informações sigilosas no contexto da Lei de Acesso à Informação.

Identificar os diferentes riscos e ameaças do ciberespaço à Segurança e à Defesa Nacional e as formas de respostas.

Identificar os efeitos das notícias falsas, das ingerências indevidas e das influências ocasionadas pelas redes sociais e mídias sociais.

Identificar as atividades de criptografia.

Identificar as atividades de certificação digital.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA
ÉTICA – PLADIS - VI - SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS

CONTEÚDO: SEGURANÇA DA INFORMAÇÃO E CIBERESPAÇO	Cg H:	EIXO TRANSVERSAL	PADRÃO DE DESEMPENHO
ASSUNTOS			
1. Fundamentos de segurança da informação. 1.1 Disponibilidade, integridade, confidencialidade e autenticidade. 1.2 Elaboração e implementação de normativos. 1.3 Noções de criptografia. 1.4 Certificação digital.	12	Atenção Seletiva Análise Raciocínio indutivo Organização Direção Proatividade Criatividade	Analisar os aspectos de confidencialidade, integridade e disponibilidade no planejamento e na implementação da segurança da informação institucional e nacional.
2. Lei Geral de Proteção de Dados (LGPD) 2.1 Impactos causados pela LGPD. 2.2 Principais conceitos, implicações, regras. 2.3 <i>Stakeholders</i> e processos envolvidos. 2.4 Exploração cibernética.	8		
3. Ambiente Informacional Digital 3.1 Sistema de Informação Nacional. 3.2 Guerra informacional e seus vetores, considerando o gerenciamento de informações e a desinformação. 3.3 Investigação, perícia e respostas cibernéticas.	10		
4. Segurança na internet. 4.1 Fundamentos de governança de Tecnologia da Informação e Comunicação, riscos e proteção. 4.2 Higiene cibernética: atuação recomendada para manter a integridade das redes e mídias sociais, segurança e ética. 4.3 Influências ocasionadas pelas redes sociais e mídias sociais. 4.4 Segurança em dispositivos móveis, em Internet das Coisas (IoT) e na internet com tecnologia 5G. 4.5 Formas de invasão de rede. 4.6 Segurança, principais desafios, privacidade e soluções no uso de dados e informações em computação na nuvem e em sistema de computação sem servidor.	17	Atenção Seletiva Análise Proatividade	Analisar os aspectos de segurança no uso da internet, seus aplicativos e suas consequências.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA
ÉTICA – PLADIS - VI - SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS

AValiação da Aprendizagem	2		
----------------------------------	---	--	--

ORIENTAÇÕES METODOLÓGICAS

1. Objetivos da Aprendizagem

Assunto 1

- Compreender os fundamentos da segurança da informação (CONCEITUAL).
- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).
- Reconhecer questões relativas à ética profissional e como ela pode ser informada por práticas políticas (FACTUAL).

Assuntos 2

- Identificar as implicações da LGPD (FACTUAL).
- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).
- Reconhecer questões relativas à exploração do ciberespaço em consonância com a LGPD (FACTUAL).

Assunto 3

- Compreender os conceitos básicos relativos ao Sistema de Informação (CONCEITUAL).
- Identificar os riscos da guerra informacional (FACTUAL).
- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).
- Identificar os riscos da desinformação usadas para manipular a opinião pública. (FACTUAL).

Assunto 4

- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).
- Identificar os tipos de ciberataques, seus riscos e suas consequências (FACTUAL).
- Identificar as formas de invasão de rede (FACTUAL).
- Compreender os conceitos básicos relativos à segurança na internet (CONCEITUAL).
- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).
- Identificar os riscos do uso da internet (FACTUAL).

2. Procedimentos Didáticos

Assunto 1 a 4 - Fornecer aos alunos textos sobre o assunto com questões para serem discutidas em plenário. A aula pode ser conduzida por professor convidado. Um tempo destinado a debate abordando as questões apresentadas.

3. Avaliação da Aprendizagem

Será conduzida com uma carga horária de 2 horas, por meio da avaliação formativa com trabalhos em grupo, produção de papers individuais e debates.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA
ÉTICA – PLADIS - VI - SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS

4. Indicações Básicas de Segurança na Atividade

Não é o caso.

REFERÊNCIAS

BRASIL. Lei nº 12.735, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares. Brasil, 2012.

_____. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal. Brasil, 2012.

_____. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasil, 2014.

_____. Lei nº 13.709, de 14 de agosto de 2018, alterada pela Lei nº 13.853, de 08 de julho de 2019. Lei Geral de Proteção de Dados Pessoais. Brasil, 2018.

_____. Lei nº 13.675, de 11 de junho de 2018. Disciplina a organização e o funcionamento dos órgãos responsáveis pela segurança pública, nos termos do § 7º do art. 144 da Constituição Federal; cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS); institui o Sistema Único de Segurança Pública (Susp); altera a Lei Complementar nº 79, de 7 de janeiro de 1994, a Lei nº 10.201, de 14 de fevereiro de 2001, e a Lei nº 11.530, de 24 de outubro de 2007; e revoga dispositivos da Lei nº 12.681, de 4 de julho de 2012. Brasil, 2018.

_____. Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Brasil, 2021.

_____. Decreto nº 19.841, de 22 de outubro de 1945. Carta das Nações Unidas. Brasil, 1945.

DONDA, Daniel. **Guia Prático de Implementação da LGPD**. São Paulo: ed. Labrador, 2020.

KIM, David; SOLOMON, Michael G. **Fundamentos de Segurança de Sistemas de Informação**. Rio de Janeiro: ed. LTC, 2014.

MACHADO, Felipe Nery Rodrigues. **Segurança da informação: Princípios e controle de ameaças**. São Paulo: ed. Érica, 2014.

MONTANARO, Domingo; GIOVA, Giuliano; BLUM Renato Opice. **Ciber Risk**. São Paulo: ed. Revista dos Tribunais, 2020.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - VII - CIBERATIVIDADES

DISCIPLINA	VII - CIBERATIVIDADES	Cg H Total: 139 h
-------------------	------------------------------	--------------------------

COMPETÊNCIA PRINCIPAL:

Atuar no campo da cibernética nos níveis político e estratégico.

UNIDADES DE COMPETÊNCIAS:

Assessorar nos estudos, planejamentos e proposições, nos níveis político e estratégico, considerando os conceitos e fundamentos da cibersegurança e ciberdefesa.

Orientar a elaboração e revisão de processos e protocolos para os níveis político e estratégico.

Assessorar nos estudos, análises, planejamentos e proposições, nos níveis político e estratégico, identificando as vulnerabilidades das infraestruturas críticas nacionais.

Assessorar nos estudos, planejamentos e proposições, nos níveis político e estratégico, considerando os *cases* de ciberincidentes, a monitoria de cenários e a defesa e guerra cibernética nas operações.

Assessorar nos estudos e planejamentos em apoio às operações militares e em situações de crises políticas, no contexto do ambiente do ciberespaço.

Identificar os efeitos de ações cibernéticas ocorridas em ambiente nacional e internacional.

Interpretar as legislações nacionais e internacionais que versam sobre cibernética.

ELEMENTOS DE COMPETÊNCIAS:

Assessorar no estabelecimento de ações políticas e estratégicas preventivas que possam mitigar ciberincidentes.

Apresentar proposições para a defesa dos interesses nacionais, fundamentadas nas definições, estratégias nacionais, paradigmas e elementos da cibersegurança e ciberdefesa, de ciberincidentes e de guerra cibernética.

Contribuir com condicionantes para potencializar e fomentar as integrações e cooperações interagências, criar os laços de confiança e estabelecer a rede de ciberproteção.

Orientar nas medidas para acionamento de centros de monitoramento, respostas rápidas aos cenários de incidentes de órgãos municipais, estaduais e federais, incluindo a Polícia Federal e o Gabinete de Segurança Institucional da Presidência da República.

Identificar as vulnerabilidades das infraestruturas diante das ciberameaças.

Conhecer as atividades do setor privado no âmbito da cibersegurança e ciberdefesa que afetam a proteção de infraestruturas críticas.

Identificar as ameaças à soberania do Estado.

Assessorar na elaboração de políticas de prevenção de ciberincidentes, para a garantia da segurança, da confidencialidade, integridade e disponibilidade da informação nas redes e no ciberespaço.

Orientar no planejamento de medidas de controle de ciber sabotagem e de extorsão envolvendo público interno.

Contribuir com proposições de medidas para a segurança das áreas de infraestruturas críticas, setores essenciais do Estado.

Assessorar o gerenciamento de risco em políticas e estratégias cibernéticas.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - VII - CIBERATIVIDADES

ELEMENTOS DE COMPETÊNCIAS (continuação):

Contribuir com estratégias gerais e setoriais, com a integração necessária dos setores envolvidos para coordenar as ações em todos os campos do poder nacional e diretrizes institucionais para garantir a segurança, antecipar-se aos ciberincidentes e para o gerenciamento das crises, no nível estratégico, garantindo a soberania do Estado.

Orientar o gerenciamento de programas e políticas focados no monitoramento, resiliência, identificação e mitigação de ciberincidentes.

Contribuir com proposições no âmbito de cibernética para a atuação colaborativa envolvendo o Ministério da Defesa, os setores estratégicos e instituições parceiras.

Contribuir para a atualização dos princípios de emprego da cibersegurança e ciberdefesa.

Identificar possíveis ações para se contrapor às ações cibernéticas no âmbito da guerra híbrida.

Conhecer casos de conflitos ocorridos que empregam as ciberatividades.

Assessorar no planejamento estratégico para a cibersegurança e ciberdefesa, considerando os ciberincidentes em crises políticas e em conflitos armados.

Identificar ações para mitigar os efeitos das notícias falsas, das ingerências indevidas e das influências ocasionadas pelas redes sociais e mídias sociais.

Induzir ações de precaução no uso de redes sociais e mídias sociais (facebook, telegram, instagram, signal, messenger twitter, youtube etc).

Assessorar na análise de risco de ciberincidentes.

Conhecer as repercussões de ciberincidentes.

Identificar a adequação da eficácia das respostas apresentadas aos ciberincidentes.

Apresentar, a partir das lições aprendidas (*cases*) e exercícios de simulação, proposições para a ciberproteção das infraestruturas críticas e para as ações preventivas e corretivas institucionais.

Identificar a estrutura de governança cibernética e os atores da ciberdefesa no âmbito nacional.

Conhecer a estrutura da ciberdefesa do Ministério da Defesa e das Forças Armadas.

Contribuir com a elaboração e revisão de políticas e estratégias nacionais/setoriais, considerando o ciberespaço.

Identificar as ações preconizadas pelos marcos normativos nacional e institucional relacionadas com o ciberespaço.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - VII - CIBERATIVIDADES

CONTEÚDO: FUNDAMENTOS DO CIBERESPAÇO	Cg H:	EIXO TRANSVERSAL	PADRÃO DE DESEMPENHO
ASSUNTOS			
1. Conceitos e fundamentos de cibersegurança e ciberdefesa. 1.1 Fundamentos do ciberespaço 1.1.1 Disponibilidade, integridade, confidencialidade e autenticidade. 1.1.2 Noções de certificação digital. 1.2 Definições, elementos e paradigmas da cibersegurança e ciberdefesa. 1.3 Capacidades operativas da cibernética: dissuasão, proteção, resiliência, investigação, exploração e ataque. 1.4 Atores cibernéticos maliciosos. 1.5 Tipos de ciberameaças. 1.6 Tipos de ciberataques. 1.7 Ações de ciberterrorismo. 1.8 Atores na cibersegurança e ciberdefesa no âmbito nacional. 1.9 Objetivos estratégicos da cibersegurança e ciberdefesa nacionais.	16	Atenção Seletiva Análise Organização	Discutir os conceitos a fim de aprimorar o autoaperfeiçoamento. Analisar os aspectos de confidencialidade, integridade e disponibilidade no planejamento e na implementação da segurança da informação institucional e nacional, considerando os tipos de ciberataques e suas consequências

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - VII - CIBERATIVIDADES

CONTEÚDO: INTELIGÊNCIA CIBERNÉTICA	Cg H:	EIXO TRANSVERSAL	PADRÃO DE DESEMPENHO
ASSUNTOS			
2. Inteligência cibernética. 2.1 Métodos de detecção, espionagem, prevenção e de resposta a ciberincidentes. 2.2 Análise de inteligência de fontes cibernéticas. 2.3 Incidentes no ambiente digital, ataques reais e seus impactos (estudo de <i>cases</i> com os detalhamentos). 2.4 Riscos da desinformação na dimensão cibernética. 2.5 Atividades ilegais com uso de páginas eletrônicas e de mídias sociais. 2.6 Análise de vulnerabilidades, riscos, ameaças e repercussões. Monitoramento do ciberespaço. 2.7 Hacktivism. Principais técnicas de ataques utilizadas por hackers e as melhores maneiras e práticas para evitá-las. Consequências em decorrência do ataque de hackers. 2.8 Prevenção e mitigação de ciberameaças e confiança digital. 2.9 Tendências de ciberameaças às infraestruturas críticas. 2.10 Gerenciamento de vulnerabilidades diante das ciberameaças às infraestruturas críticas: proteção de ativos de informações. 2.11 Desenvolvimento de ambientes seguros. 2.12 Estratégia de dissuasão no ciberespaço. 2.13 Ingerências e responsabilidades do setor privado na cibersegurança e ciberdefesa e na proteção de infraestruturas críticas. 2.14 Boas práticas de ciberproteção em infraestruturas críticas. 2.15 Inteligência Estratégica 2.16 Inteligência Artificial	24	Análise Organização Proatividade Objetividade Criatividade	Identificar os aspectos de inteligência cibernética no planejamento e na implementação de ações estratégicas e políticas no campo da cibernética. Interpretar e analisar as ações de ciberincidentes a fim de estabelecer proposições para a cibersegurança e ciberdefesa nacionais, institucionais e infraestruturas críticas.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - VII - CIBERATIVIDADES

CONTEÚDO: CULTURA COOPERATIVA NA DIMENSÃO CIBERNÉTICA	Cg H:	EIXO TRANSVERSAL	PADRÃO DE DESEMPENHO
ASSUNTOS			
3. Integração e cooperação interagências no campo do ciberespaço 3.1 Conceitos e benefícios da adoção da cultura cooperativa e práticas de configuração de interação interagências. 3.2 Métodos, modelos e ferramentas para melhoria da integração e cooperação interagências e para estabelecimento da rede de proteção cibernética. 3.3 Cooperação internacional em matéria de enfrentamento aos ilícitos cibernéticos.	8	Atenção Seletiva Análise Organização Criatividade Persuasão Cooperação	Identificar as condicionantes e suas injunções que orientam as relações entre as agências a fim de propor alianças para a proteção do ciberespaço.
4. Teoria e gerenciamento de crises cibernéticas. 4.1 Plano de contingência: respostas a incidentes e tomada de decisões no contexto digital. 4.2 Gestão de crise cibernética. 4.3 Prevenção e análise de desastres cibernéticos (resultantes dos ciberincidentes - estudo de cases). 4.4 Plano de resiliência e de restabelecimento das infraestruturas críticas atingidas pelos ciberincidentes. Análise de estabelecimento de redes de resiliência alternativas para atuarem diante dos efeitos dos ciberincidentes. 4.5 Construção de um sistema institucional de cibersegurança e ciberdefesa. 4.6 Governança, gestão de riscos e integridade, desenvolvimento de ambientes seguros e resilientes.	15	Análise Comparação Objetividade Proatividade Autoconfiança	Identificar os cenários de crise cibernética para projetar políticas e estratégias de sistemas de cibersegurança e ciberdefesa que contribuam para a estabilidade das Expressões do Poder Nacional.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - VII - CIBERATIVIDADES

CONTEÚDO: ATIVIDADES DO MINISTÉRIO DA DEFESA E CIBERESPAÇO	Cg H:	EIXO TRANSVERSAL	PADRÃO DE DESEMPENHO
ASSUNTOS			
5. Inferência do ciberespaço nas atividades do Ministério da Defesa e FFAA 5.1 Aplicação dos Fundamentos da Doutrina de Operações Conjuntas. Doutrina de Operações Conjuntas (MD30-M-01 – 1º Vol). 5.2 Programas Estratégicos das FFAA em ciberdefesa: 5.2.1. Marinha 5.2.2. Exército 5.2.3. FAB 5.3 Aplicação das normas militares de ciberdefesa. 5.4 Cibersegurança no Brasil 5.4.1. Visão geral da área de cibersegurança no Brasil. 5.4.2. Implicações dos ciberincidentes na segurança nacional -. 5.5 Guerra Cibernética e os conflitos na Era da Informação e seus efeitos. 5.6 Conflitos no mundo virtual com suporte de ciberativistas. 5.7 APTs¹ empregadas em apoio às crises ou aos conflitos armados. 5.8 Crises políticas e guerras cibernéticas, 5.9 Guerra cibernética nas Operações Conjuntas. 5.10 Cibersegurança e ciberdefesa diante das ameaças e conflitos híbridos. 5.11 Operações Interagências (MD33-M-12). 5.12 Mobilização de pessoal e material para a ciberdefesa. (Ex: SINAMOB, BID, RENER). 5.13 Estudo de <i>cases</i> de guerras cibernéticas.	30	Análise Comparação Raciocínio dedutivo Objetividade Proatividade Cooperação Criatividade	Interpretar os marcos legais do ciberespaço e a legislação do Setor da Defesa, identificando os princípios de emprego da ciberdefesa, distinguindo os níveis de decisão e atores no nível do Estado e na estrutura de ciberdefesa das Forças Armadas. Estabelecer proposições para os planejamentos político e estratégico no campo cibernético para os setores estratégicos de Defesa, inclusive com estudos para estabelecimento de alvos estratégicos. Participar das propostas para o Plano Estratégico de Emprego Conjunto das Forças Armadas, considerando a cibernética como multiplicador do poder de combate. Interpretar as teorias que orientam as ações da Defesa Civil durante guerras cibernéticas, baseando-se nas necessidades de um cenário com óbice na infraestrutura crítica de comunicações, aplicando a RENER.

¹ APT (Ing) - *Advanced and Persistent Threats* [Ameaças Persistentes e Avançadas (tecnologicamente)]

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - VII - CIBERATIVIDADES

CONTEÚDO: ATIVIDADES DE CIBERESPAÇO	Cg H:	EIXO TRANSVERSAL	PADRÃO DE DESEMPENHO
ASSUNTOS			
6. Cibersegurança e ciberdefesa dos Órgãos Governamentais	16	Atenção Seletiva Análise	Identificar as atividades dos atores na cibersegurança e ciberdefesa no âmbito nacional, localizados na Capital Federal. Estudo Interdisciplinar de Campo
7. Laboratório de crise de infraestrutura crítica	4	Atenção Seletiva	Identificar as atividades de um Laboratório de Segurança Cibernética (LaSC) do IME. Estudo Interdisciplinar de Campo
8. Crise cibernética em infraestrutura crítica (CIBERINFRA).	24	Planejamento Resolução de problemas Persuasão	Identificar as estratégias internacional e nacional referentes ao ciberespaço. Analisar políticas e estratégias do governo brasileiro aplicadas ao tema de cibersegurança e ciberdefesa, em uma situação de crise. Realizar análises e proposições, nos níveis político e estratégico, em resposta às vulnerabilidades cibernéticas de estruturas do Estado ou de infraestruturas críticas, em uma simulação de crise cibernética. Exercício de simulação de decisão estratégica.
AVALIAÇÃO DA APRENDIZAGEM	2		

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - VII - CIBERATIVIDADES

ORIENTAÇÕES METODOLÓGICAS

1. Objetivos da Aprendizagem

Assunto 1

- Compreender os fundamentos do ciberespaço relacionados à cibersegurança e ciberdefesa (CONCEITUAL).
- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).
- Identificar a ocorrência do ciberterrorismo e suas repercussões (CONCEITUAL).

Assunto 2

- Compreender os conceitos básicos relativos à inteligência cibernética (CONCEITUAL).
- Examinar os riscos e as ciberameaças com um estudo de *cases* (CONCEITUAL).
- Compreender os conceitos básicos relativos às ciberameaças (CONCEITUAL).
- Identificar as atividades ilegais da internet (FACTUAL).
- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).
- Identificar as vulnerabilidades, riscos e ameaças existentes no ciberespaço (FACTUAL).

Assunto 3

- Compreender os princípios e normatizações que regem as interações e cooperações interagências (CONCEITUAL).
- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).
- Identificar a necessidade de estabelecimento de interações e cooperações (FACTUAL).

Assunto 4

- Examinar o desenvolvimento de crises cibernéticas com um estudo de *cases* (CONCEITUAL).
- Identificar os níveis de condução da manobra de crise, as dimensões estratégicas e as etapas de desenvolvimento da crise (CONCEITUAL).
- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).

Assunto 5

- Compreender os conceitos básicos relativos aos Marcos Normativos da Defesa relacionadas ao ciberespaço (CONCEITUAL).
- Compreender o papel dos meios militares e a aplicação do poder militar nas ciberatividades (CONCEITUAL).
- Expressar seus pensamentos de modo claro, preciso e conciso (ATITUDINAL).
- Identificar e interpretar as influências da legislação na formulação das ações da Defesa, bem como na proposição de alterações na legislação (FACTUAL).

Assunto 6

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - VII - CIBERATIVIDADES

- Identificar a estrutura e as atividades dos órgãos da estrutura de Estado que tratam da cibersegurança e ciberdefesa.

Assunto 7

- Identificar a estrutura e as atividades de laboratório de crise de infraestrutura crítica do IME/Itaipu.

Assunto 8

- Planejar ações atinentes a uma manobra de crise em um estudo de caso próximo da realidade envolvendo uma crise cibernética com repercussões na área política-estratégica (PROCEDIMENTAL).
- Expressar, com facilidade (ou naturalidade), suas opiniões ou questionamentos (ATITUDINAL).
- Ser convincente em suas atitudes e palavras (ATITUDINAL).

2. Procedimentos Didáticos

Assuntos 1, 2, 3 e 4 - fornecer aos estagiários textos sobre o assunto com questões para serem discutidas em plenário. A aula pode ser conduzida por professor convidado. Um tempo destinado a debate abordando as questões apresentadas.

Assuntos 2.3 e 4.3 - fornecer aos estagiários casos de ciberataques para serem discutidos em plenário.

Assuntos 1, 2, 3, 4 e 5 - comportam aula com uma apresentação teórica complementando o estudo preliminar, enfocando os conceitos e o entendimento dos fundamentos, seguida de discussão.

Assunto 6 - consiste em Viagem de Estudos a Brasília com a finalidade de identificar a estrutura de governança e cibersegurança e os atores da ciberdefesa no âmbito nacional (ComDCiber, GSI/PR, MRE, ABIN e Polícia Federal).

Assunto 7 - consiste em Visita de Estudos ao IME com a finalidade de identificar a estrutura e atividades do laboratório de crise do IME/Itaipu.

Assunto 8 – comporta exercício de simulação de decisão estratégica “CIBERINFRA”, conduzido em atividade de grupo, focada em crise de infraestrutura crítica, a ser conduzido na sede da ESG, baseado nos exercícios Guardiã Cibernético e *Locked Shields*, com apoio do ComDCiber

3. Avaliação da Aprendizagem

Será conduzida com uma carga horária de 2 horas, por meio da avaliação somativa com trabalhos em grupo, produção de papers individuais e debates.

4. Indicações Básicas de Segurança na Atividade

Não é o caso.

REFERÊNCIAS

ANTONIO, Adriano Martins. **Segurança Cibernética: Uma Questão de Sobrevivência**. Ananindeua: ed. International Academy. 2021. Disponível: em <https://www.amazon.com.br/CISEF-Seguran%C3%A7a-Cibern%C3%A9tica-Quest%C3%A3o-Sobreviv%C3%A2ncia/dp/B097TPYCGG?asin=B095CW7WTB&revisionId=eb943cfe&format=1&depth=1>. Acesso em 24 jun 22.

ANTONUCCI, Domenic, **The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities**. Nova Jersey: ed. Wiley, 2017.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - VII - CIBERATIVIDADES

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasil, 2014.

_____. Lei nº 13.709, de 14 de agosto de 2018, alterada pela Lei nº 13.853, de 08 de julho de 2019. Lei Geral de Proteção de Dados Pessoais. Brasil, 2018.

_____. Decreto nº 19.841, de 22 de outubro de 1945. Carta das Nações Unidas. Brasil, 1945.

_____. Decreto nº 10.222, de 5 de fevereiro de 2020. Estratégia Nacional de Segurança Cibernética. Brasil, 2020.

_____. Decreto nº 10.569, de 9 de dezembro de 2020. Estratégia Nacional de Segurança de Infraestruturas Críticas. Brasil, 2020.

_____. Doutrina Militar de Defesa Cibernética. Brasil, 2014.

_____. Doutrina de Operações Conjuntas. Brasil, 2020.

_____. Estratégia Nacional de Defesa. Brasil, 2012.

_____. Estratégia Nacional de Segurança da Informação. Brasil, 2019.

_____. Livro Branco de Defesa Nacional. Brasil, 2012.

_____. Livro Verde Segurança Cibernética no Brasil. Brasil, 2010.

_____. Manual de Doutrina Glossário das Forças Armadas, Glossário de Defesa Cibernética. Brasil, 2015.

_____. Manual de Doutrina de Operações Conjuntas, MD30-M-01. Brasil, 2020.

_____. Manual de Emprego do Direito Internacional dos Conflitos Armados (DICA) nas Forças Armadas. MD34-M-03. Ministério da Defesa. Brasil, 2011.

_____. Manual de Guerra Cibernética, EB70-MC-10.232. Brasil, 2017.

_____. Manual de Operações Interagências, MD-33-M-12. Brasil, 2017.

_____. PORTARIA SECOM/MCOM Nº 5973, de 28 de junho de 2022, dispõe sobre a publicidade e o patrocínio dos órgãos e entidades integrantes do Sistema de Comunicação de Governo do Poder Executivo federal – SICOM em ano eleitoral.

_____. Política Cibernética de Defesa. Brasil, 2012.

_____. Política Nacional de Defesa. Brasil, 2012.

_____. Programa Estratégico do Exército em Defesa Cibernética. Brasil, 2020.

CANONGIA, C.; GONÇALVES, JR., A.; MANDARINO JR., R. (Orgs). Guia de Referência para a Segurança das Infraestruturas Críticas da Informação. Versão 01. 2010. Brasília: Gabinete de Segurança Institucional, 2010.

CARVALHO, P.S.M. De. O Setor Cibernético nas Forças Armadas Brasileiras. In: Desafios Estratégicos para a Segurança e Defesa Cibernética. 1ª Ed. Brasília: Presidência da República, 2011, pp. 13-34.

CENTRO DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS DE GOVERNO (CTIR Gov). Aumento de Incidentes Cibernéticos em Infraestruturas Crítica. Brasil, 2022.

_____. Tendências de ameaças cibernéticas às infraestruturas críticas. Brasil, 2021. Sites recomendados:
<https://www.nist.gov/cyberframework>;
<https://cisa.gov/cyber-incident-response>;

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - VII - CIBERATIVIDADES

<https://www.cisa.gov/infrastructure-security>;
https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/report-2021-ot-cybersecurity.pdf?utm_source=blog&utm_campaign=state-of-ot-and-cybersecurity-report;
https://www.fortinet.com/resources/cyberglossary/ot-security-best-practices?utm_source=blog&utm_campaign=ot-security-best-practices;
https://www.fortinet.com/solutions/industries/scada-industrial-control-systems/what-is-ot-security?utm_source=blog&utm_campaign=what-is-ot;
<https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services>;
<https://www.ctir.gov.br/alertas/>.

CLARKE, Richard A.; KNAKE Robert K. **O Quinto Domínio**. Rio de Janeiro: ed. Alta Books, 2021.

_____. **Guerra Cibernética: a Próxima Ameaça à Segurança e o que Fazer a Respeito**. Rio de Janeiro: ed. Brasport, 2015.

CONVENÇÃO DE BUDAPESTE - sobre o cibercrime. Budapeste, 2001.

FERNANDES, J.H.C. **Gestão da Segurança e Comunicações**. Série Segurança da Informação. 2010.

GABINETE DE SEGURANÇA INSTITUCIONAL. **Portaria 45, de 8 de setembro de 2009. Institui, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), o Grupo Técnico de Segurança Cibernética**. Brasília: publicada no DOU, 09/09/2009.

GRAUMAN, B. **Cyber-security: The vexed question of global rules**. Bruxelas: SDA – Security & Defense Agenda, 2013.

ISONI, M.M.; VIDOTTI, S.A.B.G. **E-crime em ambientes digitais informacionais da Internet**. DataGramaZero – Revista de Ciência da Informação, v.8, n.2, 2007.

GREEMBERG, Andy. **Sandworm: Uma nova era na Guerra Cibernética e a caça pelos hackers mais perigosos do Kremlin**. Rio de Janeiro: ed. Alta Books, 2022.

JASPER, Scott. **Strategic Cyber Deterrence**. Londres: ed. Rowman & Littlefield, 2017.

KENT, Sherman. **Strategic Intelligence For American World Policy**. Nova Jersey: ed. Princeton University Press, 2015.

KIM, David; SOLOMON, Michael G. **Fundamentos de Segurança de Sistemas de Informação**. Rio de Janeiro: ed. LTC, 2014.

MANDARINO JR., R.; CANONGIA, C. (Orgs.). **Livro Verde: Segurança Cibernética no Brasil**. Brasília: GSI – Gabinete de Segurança Institucional, 2010.

MITNICK. Kevin D.; VAMOS, Robert. **The Art Invisibility**. Boston: ed. Little, Brown and Company, 2017.

MARCO DE AÇÃO DE HYOGO. Disponível em: https://www.defesacivil.pr.gov.br/sites/defesa-civil/arquivos_restritos/files/documento/2018-12/MarcodeHyogoPortugues20052015.pdf. Acesso em 22 jun 22.

MARCO DE SENDAI PARA A REDUÇÃO DO RISCO DE DESASTRES 2015-2030. Disponível em: <https://www.defesacivil.pr.gov.br/Pagina/Legislacao-internacional>. Acesso em 22 jun 22.

TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS. NATO Cooperative Cyber Defence Centre of Excellence. Cambridge University Press. 2013.

O’LEARY, Mike. **Cyber Operations**. Nova Iorque: ed. Apress, 2020.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - VII - CIBERATIVIDADES

STOLL, Clifford. **The Cuckoo's EGG, Tracking a Spy Through the Maze of Computer Espionage**. Nova Iorque: ed. Pocket Books, 2005
Tallinn Manual 2.0 **On The International Law Applicable to Cyber Operations**, NATO Cooperative Cyber Defence Centre of Excellence.
Cambridge: ed. Cambridge University Press, 2017.
VIEIRA, James Batista; BARRETO, Rodrigo Tavares de Souza. **Governança, gestão de riscos e integridade**. Disponível em:
<<http://repositorio.enap.gov.br/handle/1/4281>. Acesso em 22 jun 22.
Vusacri, Alessandro. **A Guerra na Era da Informação**. São Paulo: ed. Contexto. 2018.
ZETTER, Kim. **Countdown to Zero Day**. Rio de Janeiro: ed. Brasport. 2017.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - VIII - METODOLOGIA DA PESQUISA CIENTÍFICA

DISCIPLINA	VIII - METODOLOGIA DA PESQUISA CIENTÍFICA			Cg H Total: 27 h
COMPETÊNCIA PRINCIPAL: Apresentar resultados de pesquisa científica.				
UNIDADES DE COMPETÊNCIAS: Assessorar nas atividades de pesquisa científica em Cibernética. Participar da elaboração de trabalho acadêmico no âmbito da dimensão cibernética.				
ELEMENTOS DE COMPETÊNCIAS: Atuar com uso das técnicas de coleta de dados em trabalhos individuais e em grupo. Apresentar trabalho acadêmico focado nas atividades do ciberespaço, de acordo com as normas preconizadas pela ABNT e as normas da Escola.				
CONTEÚDO: COLETA, TRATAMENTO E ANÁLISE DOS DADOS	Cg H:	EIXO TRANSVERSAL	PADRÃO DE DESEMPENHO	
ASSUNTOS				
1. Técnicas e análises.	7	Atenção seletiva Análise Organização Objetividade	Aplicar as técnicas de coleta de dados de acordo com as normas vigentes na Escola e as preconizadas pela ABNT. Apresentar resultado de estudos e pesquisas nas atividades de grupo de trabalho ou individuais.	
2. Trabalho Acadêmico.	20	Capacidade linguística Expressão escrita Objetividade Criatividade	Elaborar e apresentar trabalho acadêmico, no formato de Ensaio Acadêmico, utilizando os recursos didáticos necessários, conforme as normas vigentes na Escola e as preconizadas pela ABNT.	

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - VIII - METODOLOGIA DA PESQUISA
CIENTÍFICA

ORIENTAÇÕES METODOLÓGICAS

1. Objetivos da Aprendizagem

Assunto 1

- Compreender as formas de obtenção e utilização de dados para uma pesquisa (CONCEITUAL).
- Estruturar suas respostas em questões discursivas (ATITUDINAL).
- Apresentar o resultado de coleta de dados nos trabalhos em grupo (PROCEDIMENTAL).

Assuntos 2

- Apresentar um trabalho acadêmico (PROCEDIMENTAL).
- Ser sucinto e direto em suas explanações atingindo o núcleo do problema. (ATITUDINAL).

2. Procedimentos Didáticos

Assunto 1 - o assunto deverá ser conduzido pelo Centro do Programa de Pós-Graduação.

Assunto 2 - o trabalho acadêmico será realizado em integração ao assunto 7 do PLADIS de Estratégia do Ciberespaço. O curso não exigirá a elaboração de Trabalho de Conclusão de Curso, para fins de aprovação do estagiário. O estagiário elaborará um trabalho acadêmico, do tipo de Ensaio Teórico ou Relatório de Pesquisa sem cunho científico, a ser definido pelo Diretor do Curso.

O estagiário deverá utilizar-se do Manual para Elaboração de Trabalhos Acadêmicos da ESG.

3. Avaliação da Aprendizagem

O trabalho acadêmico será avaliado somente pelas menções: aprovado; aprovado com restrições; ou reprovado. O trabalho aprovado com restrições exigirá a retificação indicada pela comissão de avaliação.

4. Indicações Básicas de Segurança na Atividade

Não é o caso.

ESCOLA SUPERIOR DE GUERRA
CURSO SUPERIOR DE SEGURANÇA E DEFESA CIBERNÉTICA – PLADIS - VIII - METODOLOGIA DA PESQUISA
CIENTÍFICA

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. **NBR 14724: Informação e documentação - Trabalhos Acadêmicos – Apresentação**. Rio de Janeiro, 2011.

_____, **NBR 6021: Normalização e Padronização**. Rio de Janeiro, 2018.

_____, **NBR 6023: Informação e documentação - Referências – Elaboração**. Rio de Janeiro, 2002.

CREMA, Roberto. **Além das disciplinas: reflexões sobre transdisciplinaridade geral**. São Paulo: ed. Summus, 1993.

DEMO, Pedro. **Introdução à metodologia da ciência**. São Paulo: ed. Atlas., 1985.

_____, **Conhecimento Moderno - sobre ética e intervenção do conhecimento**. Petrópolis: ed. Vozes, 1998.

ENSAIO ACADÊMICO. Disponível em: <https://trilhante.com.br/trilha/fdrp/sobre/ensaio-academico>. Acesso em 23 jun 22.

ESCOLA SUPERIOR DE GUERRA. **Manual para Elaboração de Trabalhos Acadêmicos**. Rio de Janeiro: ESG, 2024.

FERRARI, A. T. **Metodologia da Pesquisa Científica**. São Paulo: ed. The Grow-Hill, 1986.

GALLIANO, A. Guilherme. **O método científico - teoria e prática**. São Paulo: ed. Harbra, 1979.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. São Paulo: ed. Atlas, 1988.

KERLINGER, Fred N. **Metodologia da pesquisa em ciências sociais - um tratamento conceitual**. Ed. EPU / EDUSP. São Paulo, 1980.

_____. **Métodos e técnicas de pesquisa social**. São Paulo: ed. Atlas., 1987.

MIRANDA, José Luís Carneiro de. **Artigo Científico: estrutura e redação**. Niterói: ed. Intertexto, 2000.

MORIN, Edgard. **Ciência com consciência**. Rio de Janeiro: ed. Bertrand Brasil, 1996.

NEIVA, Eduardo. **O racionalismo crítico de Popper**. Rio de Janeiro: ed. Francisco Alves, 1999.

ORIENTAÇÕES PARA ENSAIO ACADÊMICO. Disponível em:
<file:///E:/LEGISLA%C3%87%C3%95ES/LEGISLA%C3%87%C3%83O%20ESG/trabalhos%20acad%C3%AAmcos%20normas/Orienta%C3%A7%C3%B5es%20para%20o%20Ensaio%20Acad%C3%AAmico%20IEB.pdf>. Acesso em 23 jun 22.

POPPER, Karl R. **Conjecturas e Refutações. Coleção Pensamento Científico**. Brasília: ed. Universidade de Brasília, 1972.