Universidade Federal Fluminense

Instituto de Computação

Segurança Cibernética no Setor Marítimo

Desafios e Oportunidades de Pesquisa e Desenvolvimento

Prof. Raphael Machado

I Painel Sobre Segurança Cibernética no Setor Marítimo, 17-dez-2020

Pesquisa com participantes: https://forms.gle/qnN1xbNxLnQqQVsX6

Raphael Machado

- Professor do Instituto de Computação da UFF
  - Docente do Programa de Pós-Graduação em Computação
- Atuação em Segurança desde 2003 (e em TI desde 19??)
- Pesquisador em Computação (D.Sc. 2010, PQ-1D, JCNE)
- Eventos: SegInfo, WRAC+, SBSeg, IEEE MetroInd
- Diversos projetos de pesquisa básica e aplicada

www.linkedin.com/in/raphael-cs-machado

Setor Marítimo e Espaço Cibernético

Definindo o ponto de vista desta breve apresentação


Setor Marítimo?

Espaço Cibernético?


Indústria Naval
Transporte
Defesa
Setor Marítimo =)
Pesca
Pesquisa
Meio-Ambiente
Óleo&Gás

Setor Marítimo: Importância Global

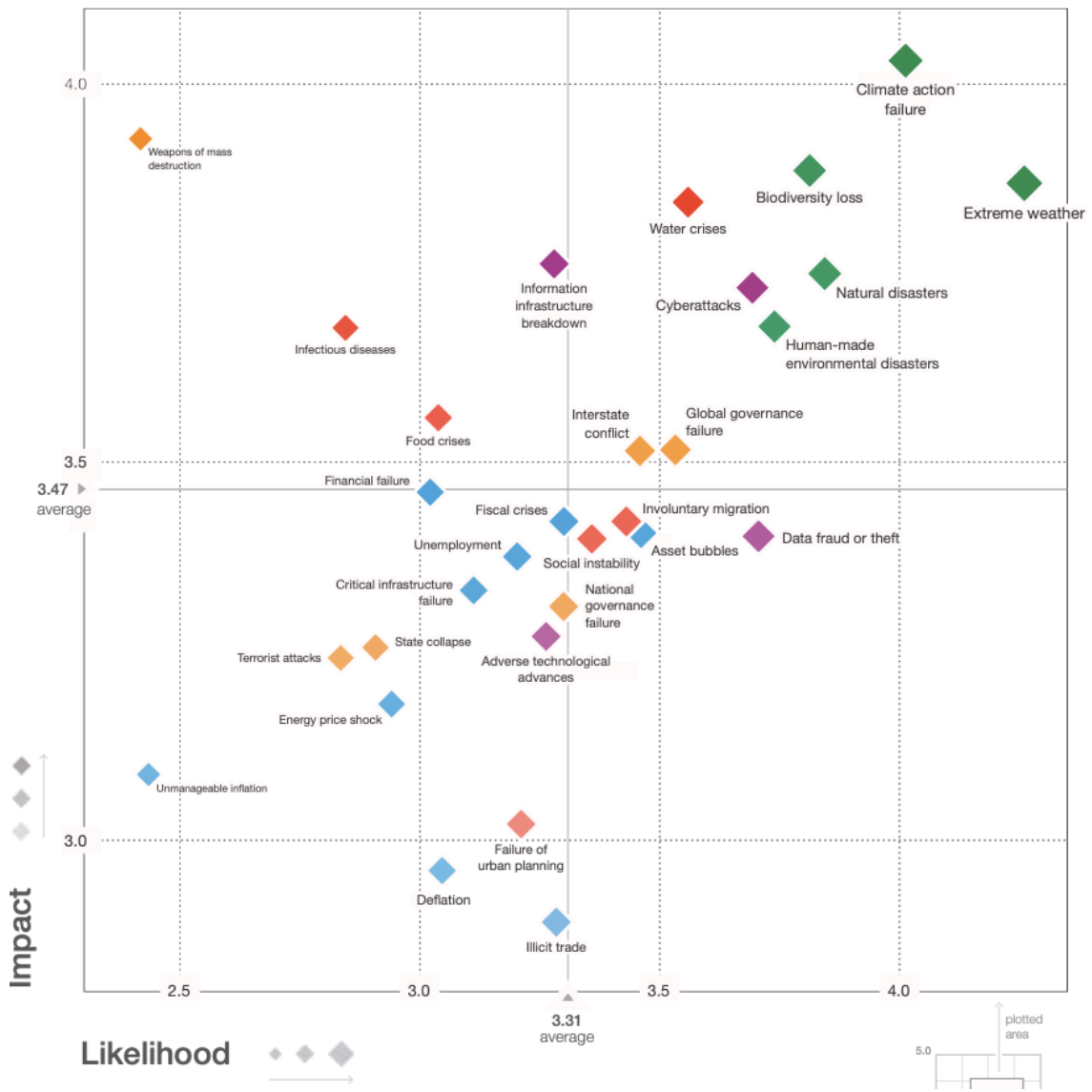
- 90% do comércio internacional
- 11 bilhões de toneladas de cargas
- 14 trilhões de dólares transportados

Setor Marítimo: Vocação Brasileira

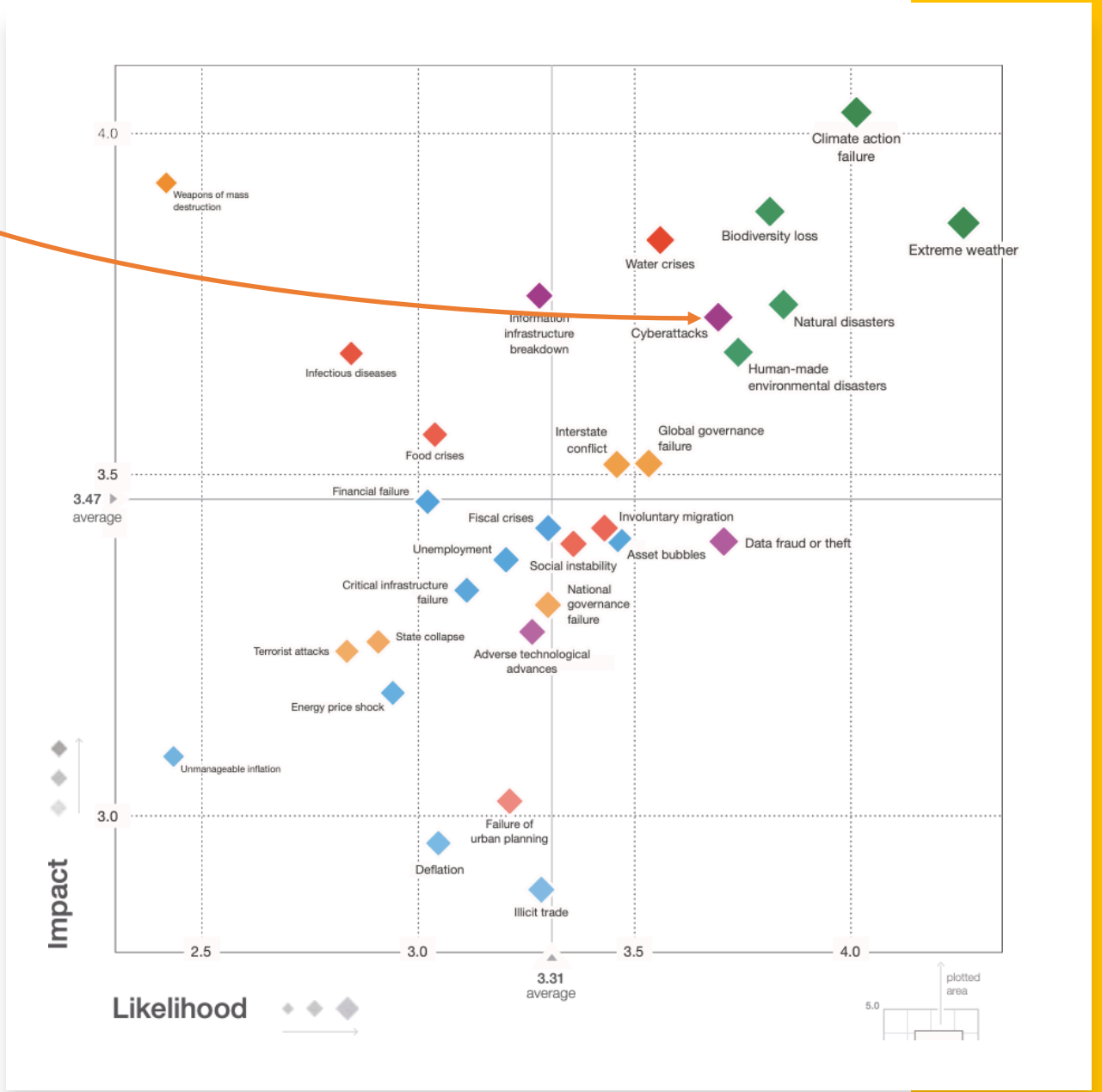
- 7.400km de costa
- 5.700.000km^2 de jurisdição marítima (Amazônia Azul)
- Faixa de 200km da costa concentra
  - cerca de 78% da produção (receitas)
  - 93% das indústrias
  - 80% da população
  - principais cidades, usando 85% da eletricidade consumida no país
- Mais de 95% do comércio internacional brasileiro é transportado por mar – mais de US$400bi/ano
- 191 portos privados e 37 portos públicos
- Brazil responde por quase 10% do comércio marítimo global

Porém...

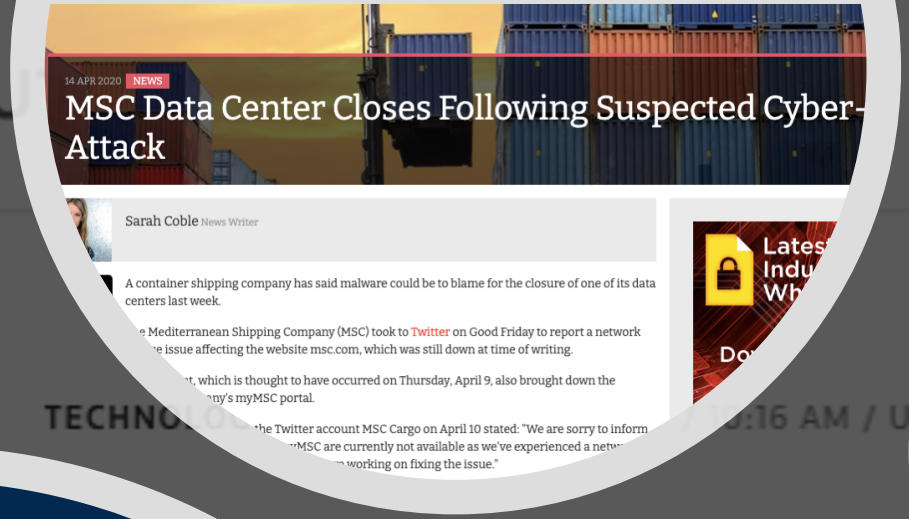
WEF Global Risks Report: Ataques Cibernéticos são risco crítico

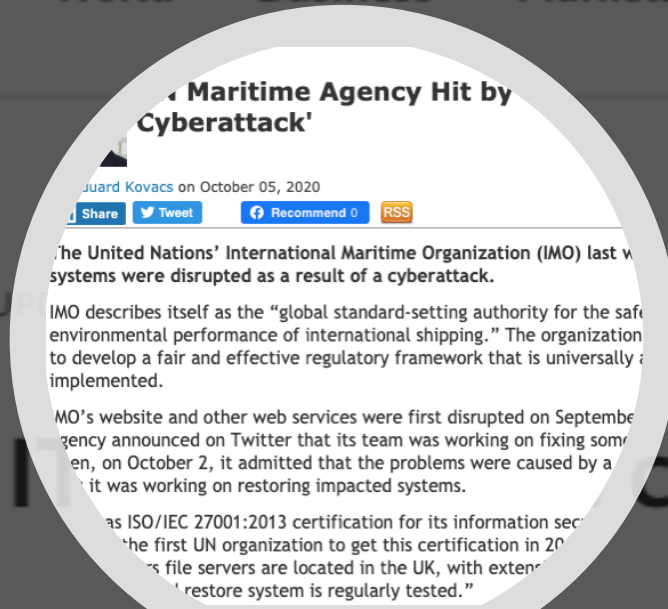


WEF Global Risks Report: Ataques Cibernéticos são risco crítico



Ataques Cibernéticos alcançam o Setor Marítimo





Normativos IMO para Segurança Cibernética

IMO INTERNATIONAL MARITIME ORGANIZATION

E

4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telephone: +44 (0)20 7735 7611 Fax: +44 (0)20 7587 3210

MSC-FAL.1/Circ.3
5 July 2017

GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

1 The Facilitation Committee, at its forty-first session (4 to 7 April 2017), and the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), having considered the urgent need to raise awareness on cyber risk threats and vulnerabilities, approved the *Guidelines on maritime cyber risk management*, as set out in the annex.

2 The Guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.

3 Member Governments are invited to bring the contents of this circular to the attention of all stakeholders concerned.

4 This circular supersedes the interim guidelines contained in MSC.1/Circ.1526.

***

ANNEX 10

RESOLUTION MSC.428(98)
(adopted on 16 June 2017)

MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS

THE MARITIME SAFETY COMMITTEE,

RECOGNIZING the urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks,

RECOGNIZING ALSO that Administrations, classification societies, shipowners and ship operators, ship agents, equipment manufacturers, service providers, ports and port facilities, and all other maritime industry stakeholders should expedite work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities,

BEARING IN MIND MSC-FAL.1/Circ.3 on *Guidelines on maritime cyber risk management* approved by the Facilitation Committee, at its forty-first session (4 to 7 April 2017), and by the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), which provides high-level recommendations for maritime cyber risk management that can be incorporated into existing risk management processes and are complementary to the safety and security management practices established by this Organization,

RECALLING resolution A.741(18) by which the Assembly adopted the International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code) and recognized, inter alia, the need for appropriate organization of management to enable it to respond to the need of those on board ships to achieve and maintain high standards of safety and environmental protection,

NOTING the objectives of the ISM Code which include, inter alia, the provision of safe practices in ship operation and a safe working environment, the assessment of all identified risks to ships, personnel and the environment, the establishment of appropriate safeguards, and the continuous improvement of safety management skills of personnel ashore and aboard ships,

1 AFFIRMS that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code;

2 ENCOURAGES Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021;

3 ACKNOWLEDGES the necessary precautions that could be needed to preserve the confidentiality of certain aspects of cyber risk management;

4 REQUESTS Member States to bring this resolution to the attention of all stakeholders.

***

Normativos IMO para Segurança Cibernética

IMO INTERNATIONAL MARITIME ORGANIZATION

4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telephone: +44 (0)20 7735 7611 Fax: +44 (0)20 7587 3210

E

MSC-FAL.1/Circ.3
5 July 2017

GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

1 The Facilitation Committee, at its forty-first session (4 to 7 April 2017), and the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), having considered the urgent need to raise awareness on cyber risk threats and vulnerabilities, approved the *Guidelines on maritime cyber risk management*, as set out in the annex.

2 The Guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.

3 Member Governments are invited to bring the contents of this circular to the attention of all stakeholders concerned.

4 This circular supersedes the interim guidelines contained in MSC.1/Circ.1526.

***

ANNEX 10

RESOLUTION MSC.428(98)
(adopted on 16 June 2017)

MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS

THE MARITIME SAFETY COMMITTEE,

RECOGNIZING the urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks,

RECOGNIZING ALSO that Administrations, classification societies, shipowners and ship operators, ship agents, equipment manufacturers, service providers, ports and port facilities, and all other maritime industry stakeholders should expedite work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities,

BEARING IN MIND MSC-FAL.1/Circ.3 on *Guidelines on maritime cyber risk management* approved by the Facilitation Committee, at its forty-first session (4 to 7 April 2017), and by the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), which provides high-level recommendations for maritime cyber risk management that can be incorporated into existing risk management processes and are complementary to the safety and security management practices established by this Organization,

RECALLING resolution A.741(18) by which the Assembly adopted the International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code) and recognized, inter alia, the need for appropriate organization of management to enable it to respond to the need of those on board ships to achieve and maintain high standards of safety and environmental protection,

NOTING the objectives of the ISM Code which include, inter alia, the provision of safe practices in ship operation and a safe working environment, the assessment of all identified risks to ships, personnel and the environment, the establishment of appropriate safeguards, and the continuous improvement of safety management skills of personnel ashore and aboard ships,

1 AFFIRMS that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code;

2 ENCOURAGES Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021;

3 ACKNOWLEDGES the necessary precautions that could be needed to preserve the confidentiality of certain aspects of cyber risk management;

4 REQUESTS Member States to bring this resolution to the attention of all stakeholders.

***

Normativos IMO para Segurança Cibernética

IMO INTERNATIONAL MARITIME ORGANIZATION

E

4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telephone: +44 (0)20 7735 7611 Fax: +44 (0)20 7587 3210

MSC-FAL.1/Circ.3
5 July 2017

GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

1 The Facilitation Committee, at its forty-first session (4 to 7 April 2017), and the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), having considered the urgent need to raise awareness on cyber risk threats and vulnerabilities, approved the *Guidelines on maritime cyber risk management*, as set out in the annex.

2 The Guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.

3 Member Governments are invited to bring the contents of this circular to the attention of all stakeholders concerned.

4 This circular supersedes the interim guidelines contained in MSC.1/Circ.1526.

***

ANNEX 10

RESOLUTION MSC.428(98)
(adopted on 16 June 2017)

MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS

THE MARITIME SAFETY COMMITTEE,

RECOGNIZING the urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks,

RECOGNIZING ALSO that Administrations, classification societies, shipowners and ship operators, ship agents, equipment manufacturers, service providers, ports and port facilities, and all other maritime industry stakeholders should expedite work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities,

BEARING IN MIND MSC-FAL.1/Circ.3 on *Guidelines on maritime cyber risk management* approved by the Facilitation Committee, at its forty-first session (4 to 7 April 2017), and by the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), which provides high-level recommendations for maritime cyber risk management that can be incorporated into existing risk management processes and are complementary to the safety and security management practices established by this Organization,

RECALLING resolution A.741(18) by which the Assembly adopted the International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code) and recognized, inter alia, the need for appropriate organization of management to enable it to respond to the need of those on board ships to

ronmental protection,

ter alia, the provision of safe practices
assessment of all identified risks to
nt of appropriate safeguards, and the
personnel ashore and aboard ships,

ent system should take into account
tives and functional requirements of

that cyber risks are appropriately
an the first annual verification of the
21;

that could be needed to preserve the
ent;

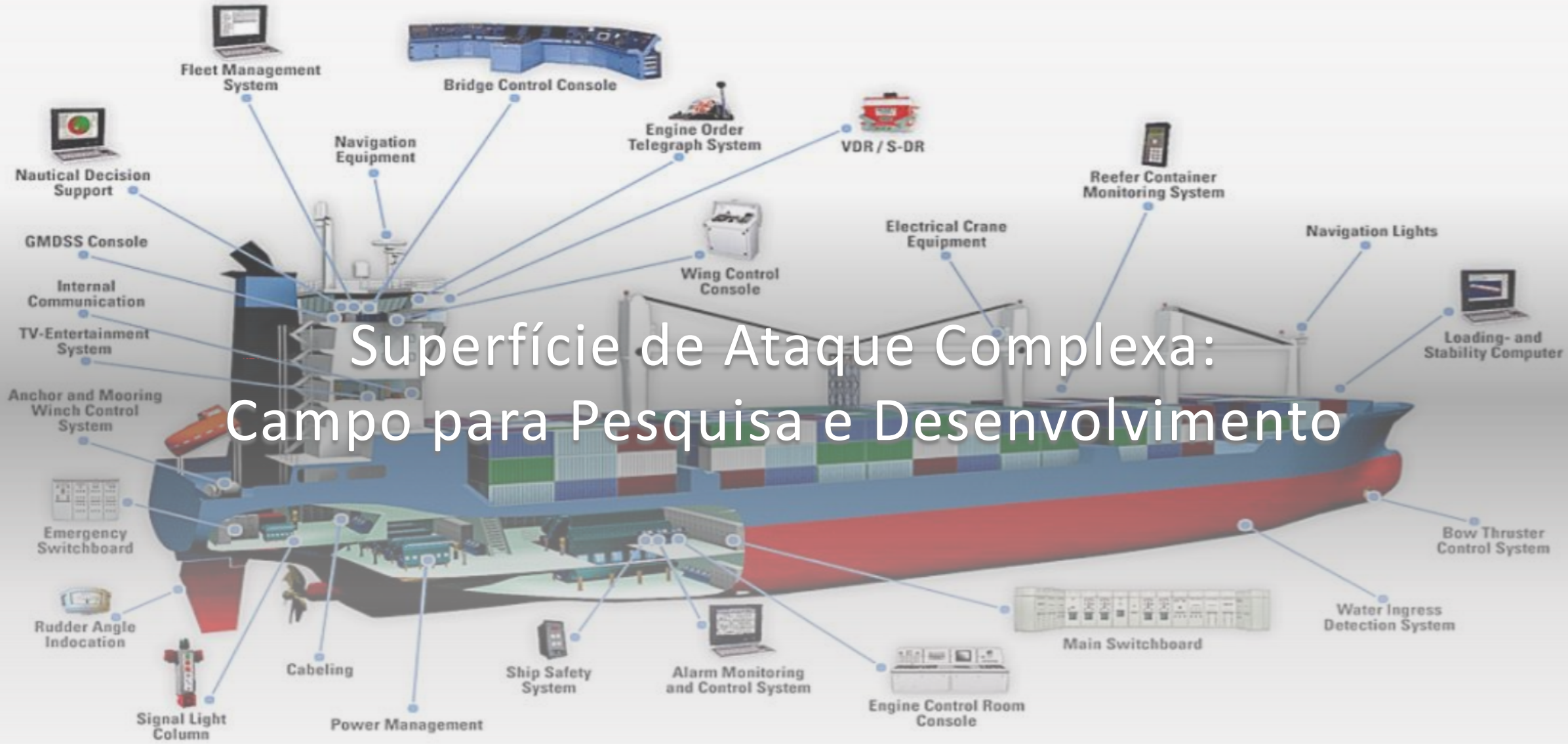
tion to the attention of all stakeholders.

1 AFFIRMS that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code;

2 ENCOURAGES Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021;

3 ACKNOWLEDGES the necessary precautions that could be needed to preserve the confidentiality of certain aspects of cyber risk management;

4 REQUESTS Member States to bring this resolution to the attention of all stakeholders.



Superfície de Ataque Complexa: Campo para Pesquisa e Desenvolvimento

Contracting Authority: European Commission H2020

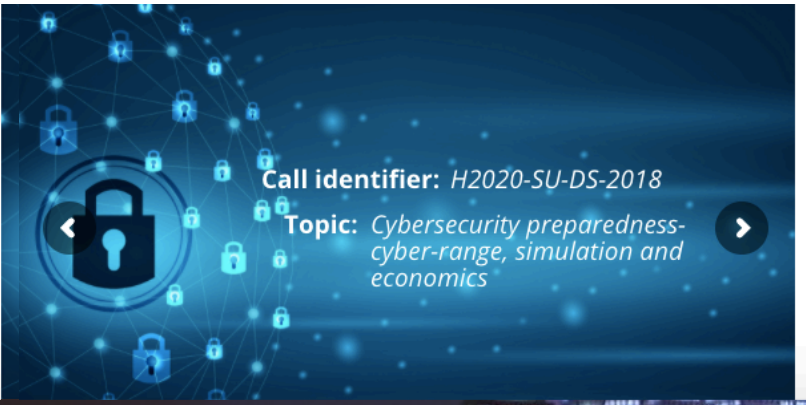
Contract Number: 833389

Starting Date: 01/09/2019

End Date: 31/08/2022

EC Funding: 6 018 367.507 €

Project Coordinator: Dr. Angelos Amditis, ICCS (A.Amditis@iccs.gr)



Cyber-MAR is an effort to fully unlock the value of the maritime logistics value chain via the development of **environment** adapting in the peculiarities of the mariti the same time easily applicable in other transport sub of innovative technologies are the technology enabler **MAR platform**, which is not only a **knowledge-based** importantly a **decision support tool** to cybersecurity n novel **risk analysis** and **econometric models**. CSIRTs/ be analysed and feed the knowl scenarios and

IBM and Port of LA announce new $6.8M cyber centre

Thursday, 10 December 2020 | Communications & Cyber Security

IBM Security and the Port of Los Angeles have announced a $6.8 million, three-year agreement to design and operate a Port Cyber Resilience Centre (CRC).

Investimentos em Pesquisa...

Tópicos e Objetivos de Pesquisa

- Análise de **Riscos e Vulnerabilidades dos Sistemas** de embarcações (IT e OT).
- Análise de **Ameaças Relacionadas às Operações** de embarcações e à tomada de decisão.
- Análise de **Ameaças à Cadeia de Produção e Suprimentos** do Setor Marítimo
- **Segurança Cibernética de Objetos Autônomos**: veículos marítimos, portos e estruturas offshore
- **Treinamentos e Processos** para proteção de marinheiros e embarcações contra ataques
- Estudo e compreensão de **Aspectos Psicológicos** relacionados a ataques (percepção e resposta)
- Desenvolvimento de **Estratégias de Recuperação** de eventos de ataque cibernético
- Análise das **Interações Cibernéticas e Ciber-Físicas** entre porto e embarcação
- Compilação de Corpo de Conhecimentos sobre **Ameaças Cibernéticas ao Setor Marítimo**.

Grupo de Pesquisa SICCCiber

Segurança da Informação, das Comunicações, dos Computadores e do Espaço Cibernético

Grupo de Pesquisa SICCCiber

SICCCIBER - SEGURANÇA DA INFORMAÇÃO, DAS COMUNICAÇÕES, DOS COMPUTADORES E DO ESPAÇO CIBERNÉTICO

Identificação

Dados do grupo

Ajuda ?

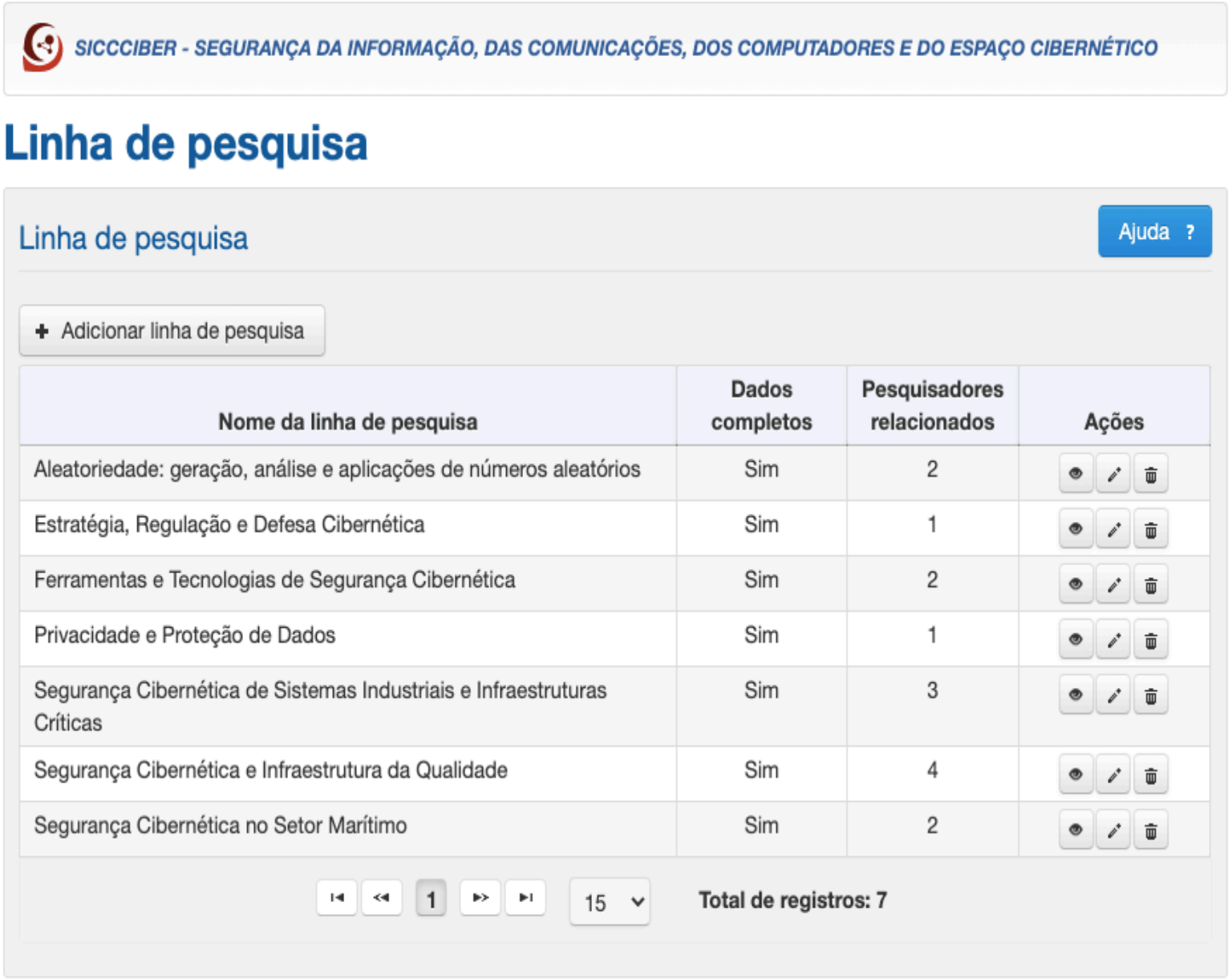
*Nome do grupo	SICCCiber - Segurança da Informação, das Comunicações, dos Computadores e do E
*Ano de formação	2010
*Instituição do grupo	Universidade Federal Fluminense
Unidade	
*Grande área predominante	Ciências Exatas e da Terra
*Área predominante	Ciência da Computação

Líderes do grupo

*Primeiro líder	Raphael Carlos Santos Machado

http://dgp.cnpq.br/dgp/espelhogrupo/3209338899543798

Grupo de Pesquisa SICCCiber



Linha de Pesquisa CiberMar

- Pesquisas iniciais com foco em Defesa (parceria com professores da Marinha do Brasil)
- Foco crescente em Mercante, Portos etc.
- Linha de pesquisa ainda em estruturação
  - Atualmente, dois pesquisadores e dois alunos (mestrado e doutorado)
  - Fortemente relacionada à linha de "Infraestruturas Críticas"

Doutorado Acadêmico para Inovação

Parceria UFF/Clavis/CNPq

- Programa Doutorado Acadêmico para a Inovação
- Objetivo: fomentar pesquisas (tese de doutorado) em temas de interesse direto do Setor Produtivo Privado
- Arranjo
  - CNPq fornece bolsa de estudo
  - Universidade oferece vaga (e orientador)
  - Empresa propõe tema e apoia o projeto

Parceria UFF/Clavis/CNPq

Universidade Federal Fluminense
Instituto de Computação
Pós-graduação em Computação

Telefone: (21) 2629-2963/2964
E-mail: secretaria.pos@ic.uff.br

EDITAL - DOUTORADO DAI 2020

O Coordenador do Programa de Pós-Graduação em Computação (PGC) do Instituto de Computação da Universidade Federal Fluminense, considerando o que estabelece a Resolução 02/2010 do Conselho de Ensino e Pesquisa e conforme estabelecido na Chamada Pública CNPq Nº 12/2020 – Programa Doutorado Acadêmico para Inovação (DAI) e na resolução Nº 7 de 09 de abril de 2020 do CNPq, faz saber que estarão abertas as inscrições para a seleção **candidatos brasileiros ou estrangeiros** ao Curso Doutorado *stricto sensu* em Computação, como Bolsistas de Doutorado na modalidade de bolsa DAI / CNPq, para o primeiro semestre do ano letivo de 2021, na forma do presente edital.

O Programa DAI busca fortalecer a pesquisa, o empreendedorismo e a inovação nas Instituições Científicas, Tecnológicas e de Inovação (ICT), por meio do envolvimento de estudantes de doutorado em projetos de interesse do setor empresarial, mediante parceria com Empresas. Dessa forma, o Programa DAI busca contribuir para o aumento da capacidade inovadora, da competitividade das empresas e do desenvolvimento científico e tecnológico no País, ao mesmo tempo em que pretende fortalecer os Sistemas Regionais de Inovação.

1. Inscrições

Formulário eletrônico: http://posgrad.ic.uff.br/inscricoes
Contato: Coordenação de Pós-Graduação em Computação
Instituto de Computação, 4º andar
Av. Gal. Milton Tavares de Souza, s/nº
Campus da Praia Vermelha
Boa Viagem
Niterói, Rio de Janeiro 24210-346
Email: secretaria.pos@ic.uff.br
Prazo: 30/11/2020 a 15/01/2021

2. Documentação

a) Formulário eletrônico de inscrição;
b) Mínimo de duas cartas de referência, enviadas por meio de formulário eletrônico, enviado por email para os avaliadores;
c) Histórico escolar;
d) Cópia frente e verso do diploma ou certificado de conclusão de curso de graduação, e do diploma ou certificado de conclusão do Mestrado. Concluintes poderão apresentar, exclusivamente para efeito de inscrição, uma declaração de que deverão concluir o curso no período letivo corrente;
e) *Curriculum Vitae*;
f) Cópia da carteira de identidade e do CPF (para brasileiros) ou passaporte (para estrangeiros);
g) Plano de Trabalho do Candidato elaborado conjuntamente com o orientador pretendido do PGC, e em conformidade com um dos temas de interesse de uma das empresas parceiras, conforme Anexo I. O plano de trabalho deve indicar explicitamente a qual dos temas do edital ele se relaciona. A adequação do Plano de Trabalho ao tema do projeto de interesse será relevante para a seleção.
h) Resultado do exame POSCOMP (fortemente recomendado, mas não obrigatório).

2. **Tema "Transformação Digital e Segurança Cibernética no Setor Marítimo", bolsa DAI cujo projeto será desenvolvido com a empresa Clavis Segurança da Informação.**

Descrição: O projeto tem por objetivo o estudo e o desenvolvimento de novas ferramentas e métodos para aumentar a eficiência e a segurança do Setor Marítimo. O Setor Marítimo é essencial para o Comércio Internacional. Anualmente, cerca de 11 bilhões de toneladas de cargas num valor total da ordem de 14 trilhões de dólares, são movimentadas por petroleiros, graneleiros, porta-contêineres e outros tipos de embarcações, respondendo por cerca de 90% do comércio internacional (International Chamber of Shipping). Nos últimos anos, a Transformação Digital vem mudando a forma como o setor atua, impactando na operação de portos e embarcações. No entanto, ao mesmo tempo em que a Transformação Digital do Setor Marítimo abre espaço para um grande aumento de eficiência com relevantes impactos econômicos, sociais e ambientais, a conectividade dos equipamentos e sistemas de portos e navios abre oportunidades para ações maliciosas por meio de um vasto conjunto de ameaças cibernéticas. O presente projeto pretende avaliar de forma conjunta as oportunidades e ameaças cibernéticas criadas pela Transformação Digital do Setor Marítimo.

- Maiores informações com o Prof. Raphael Machado (raphaelmachado@ic.uff.br)

http://www.ic.uff.br/index.php/pt/pos-graduacao/noticias-pos/1235-processo-seletivo-para-doutorado-dai-2020

Sobre o IC e o PPGC

Sobre o IC e o PPGC

Instituto de Computação

65 Docentes

3 cursos superiores

1 Programa de Pós-Graduação

Cerca de 2000 alunos

Programa de Pós-Graduação em Computação

44 Docentes

168 Teses e 566 Dissertações

Conceito CAPES 6 (Excelência)

Obrigado!!!

Raphael C S Machado
raphaelmachado@ic.uff.br

www.linkedin.com/in/raphael-cs-machado