I Painel sobre Segurança Cibernética no Setor Marítimo

O Domínio Cibernético e as Ameaças Digitais no Ambiente Naval

Alan Oliveira de Sá

17/12/2020

Sobre mim

- Doutor em Informática (UFRJ)
  área de sistemas complexos adaptativos
- Desenvolve pesquisa nas áreas de:
  - segurança cibernética
  - sistemas navais
  - sistemas de defesa
  - sistemas de controle industrial
  - sistemas inteligentes
- Colaboro em pesquisas do grupo SICCCiber (UFF)

Sumário

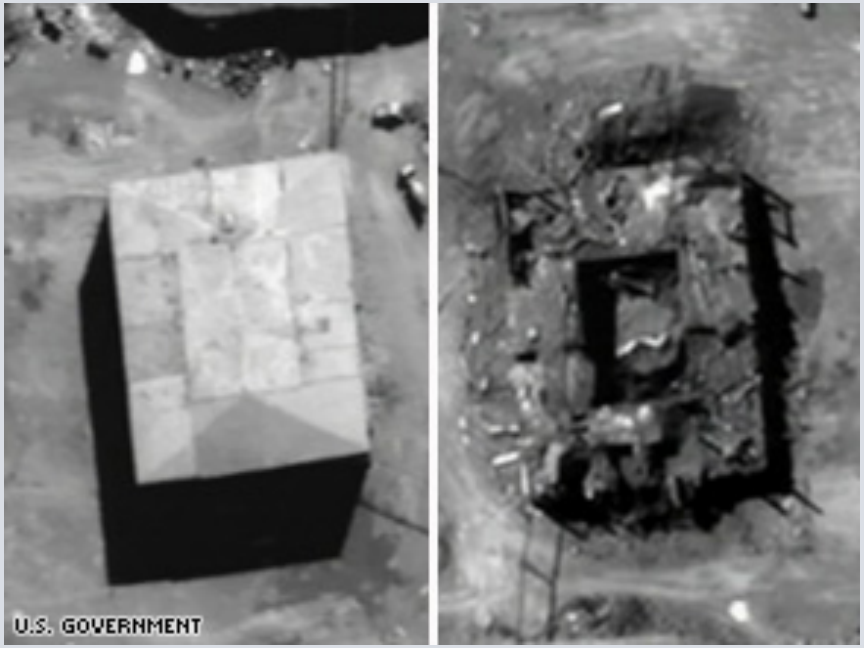
- Casos de Referência
- O Domínio Cibernético no Ambiente Naval
- Ameaças Digitais no Ambiente Naval
- Conclusões

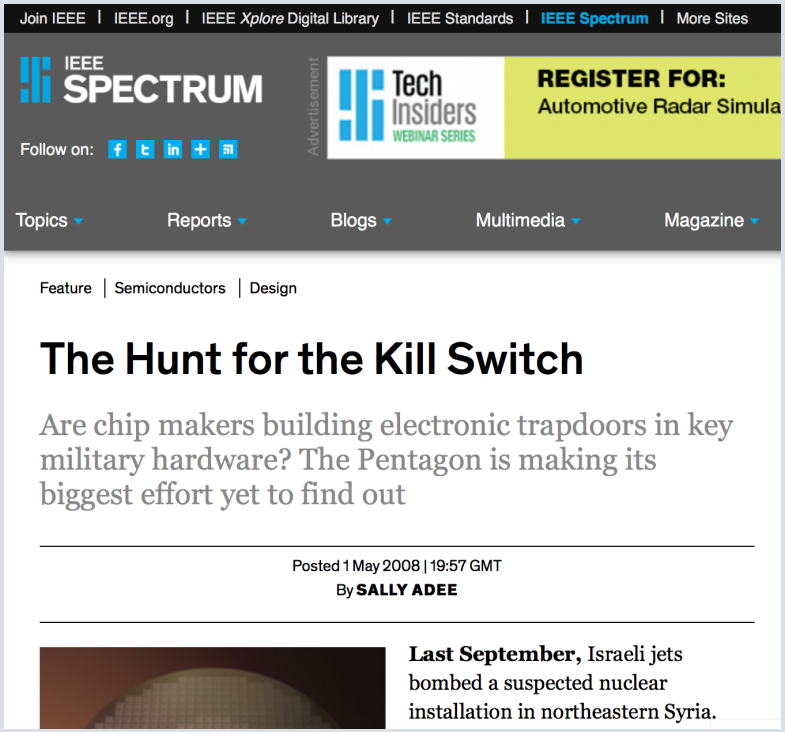
Casos de Referência

Casos de Referência

- Operação Orchard - Síria (2007)

Jatos israelenses bombardearam uma instalação nuclear suspeita no nordeste da Síria. Uma fábrica que estava sendo construída com Norte Coreanos.[1]





[1] CLARKE, Richard A., KNAKE, Robert K. **Guerra Cibernética: A próxima ameaça à segurança nacional e o que fazer sobre isso.** Brasport, 2015 (edição brasileira) 2010 (original).

[2] ADEE, Sally. **The hunt for the kill switch**. IEEE SpEctrum, v. 45, n. 5, p. 34-39, 2008.

Casos de Referência

- *Mobile Offshore Drilling Unit* (MODU) – Golfo do México (2013)[4]

  - Causa:
    - USB infectado com vírus
  - Consequências:
    - Comprometimento de computadores e sistemas operacionais
    - Paralisação de uma plataforma de petróleo
    - Perda de comunicação com sistema de navegação
    - Imobilização do propulsor
    - Deriva

[4] HAYES, Christopher R. **Maritime cybersecurity: the future of national security**. 2016. Dissertação de Mestrado. Monterey, California: Naval Postgraduate School.

Casos de Referência

- GPS de embarcações pesqueiras – Coréia do Sul (2016)[5,6]

- 280 embarcações afetadas
- GPS sinal foi bloqueado por *hackers*
- *Localização das embarcações em terra*
- Disponibilidade (modelo CIA) dos equipamentos de navegação foi interrompida
- Embarcações tiveram que retornar ao porto

[5] MIRANDA SILGADO, David. **Cyber-attacks: a digital threat reality affecting the maritime industry**. 2018.

[6] Saul, J. (2017, August). **Cyber Threats prompt return of radio for ship navigation**. Reuters. Retrieved from: https://www.reuters.com/article/us-shipping-gpscyber-idUSKBN1AN0HT

Casos de Referência

- *The Big Hack* (2015)[7]

Supply chain attack *– reportado pela Amazon.com Inc. às autoridades dos EUA.*

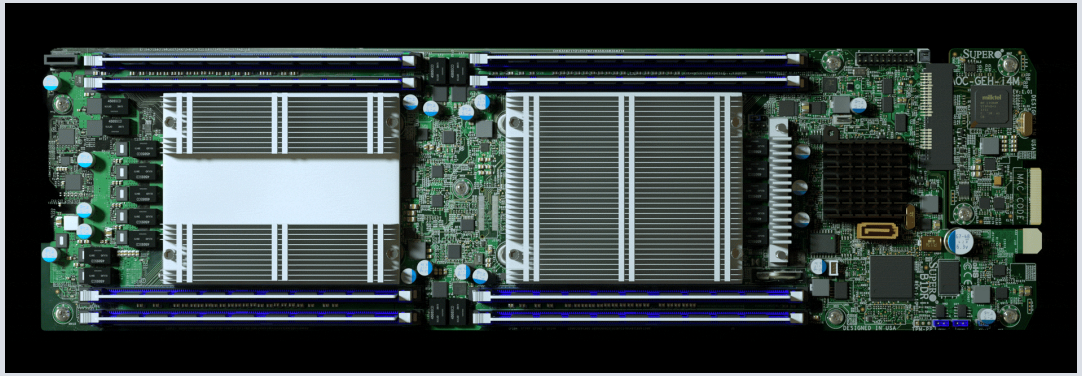
Minúsculo microchip, escondido em placas-mãe de servidores.

Entrada furtiva em redes.

Investigações: inseridos em fábricas controladas por empresas subcontratadas na China

Sistemas críticos comprometidos:

- *centros de dados do DoD dos EUA,*
- *sistemas de operação de drones da CIA; e*
- *redes em* ***navios de guerra da US Navy***



[7] ROBERTSON, J.; RILEY, M. **The Big Hack**: How China Used a Tiny Chip to Infiltrate U.S. Companies. Bloomberg Businessweek

Casos de Referência

Elementos que podem ser aplicados ao ambiente naval

Operação Orchard (2007)
Radar
Supply Chain Attack

MODU (2013)
Sistemas de Navegação
Sistema ciberfísico
Air Gap

“*The big hack*” (2015)
Supply chain attack
Redes de navios

GPS (2016)
Sensor
Sistema de Navegação
Espectro Eletromagnético

O Domínio Cibernético no Ambiente Naval

O Domínio Cibernético no Ambiente Naval

Guerra Cibernética:

"... combinação de ataques, defesas e operações técnicas especiais em redes de computadores."(PARKS; DUGGAN, 2011)

Um mundo cibernético:

"... qualquer realidade virtual contida em um conjunto de computadores e redes." (PARKS; DUGGAN, 2011)

Domínio da guerra cibernética:

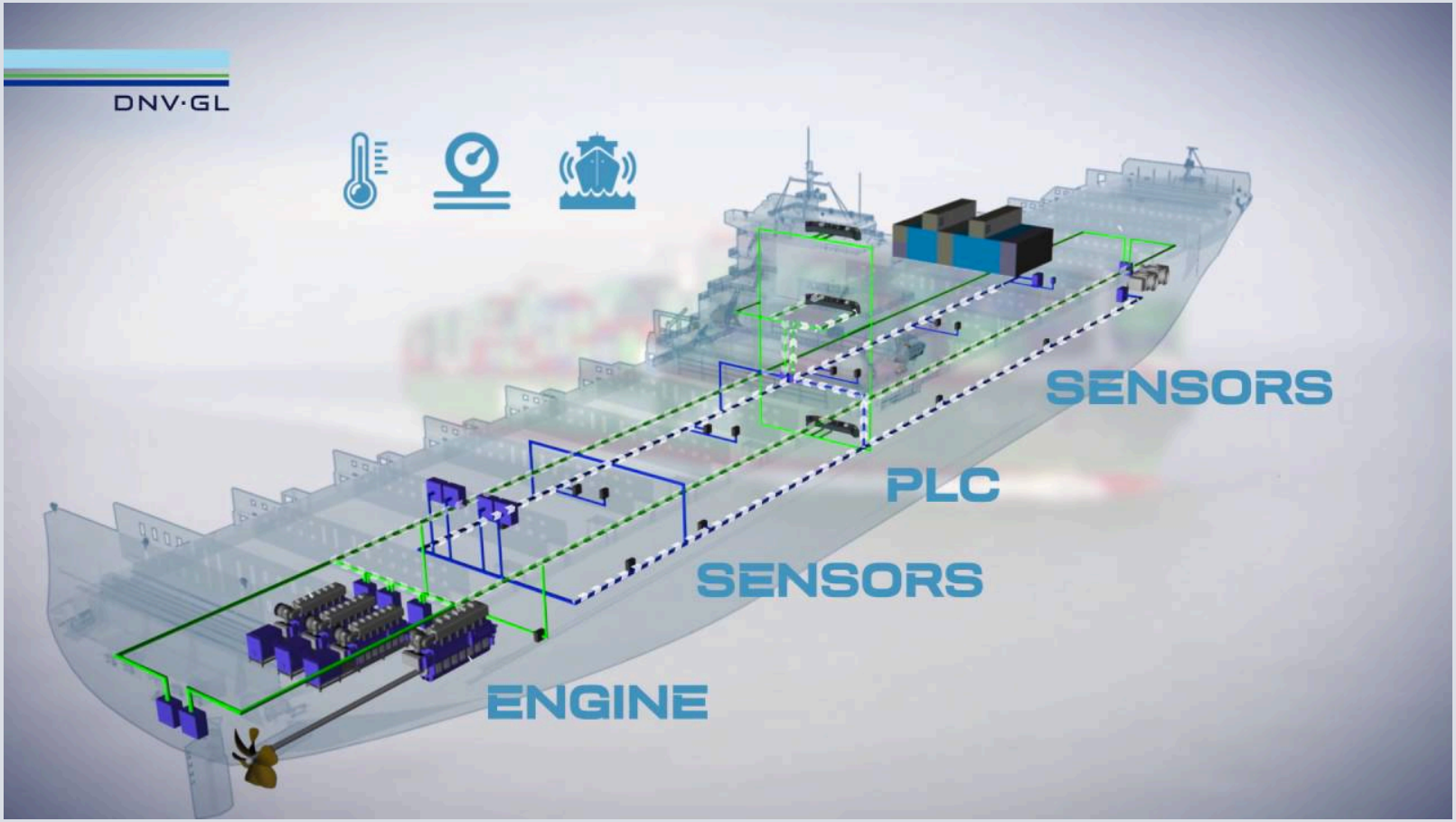
Ambiente composto por todos os mundos cibernéticos existentes.

[8] PARKS, Raymond C.; DUGGAN, David P. **Principles of cyberwarfare**. IEEE Security & Privacy, v. 9, n. 5, p. 30-35, 2011.

O Domínio Cibernético no Ambiente Naval

- Os sistemas marítimos estão seguindo as tendências mundiais e aderindo às tecnologias de:

Indústria 4.0 **Internet das Coisas (IoT)** **sensores inteligentes**



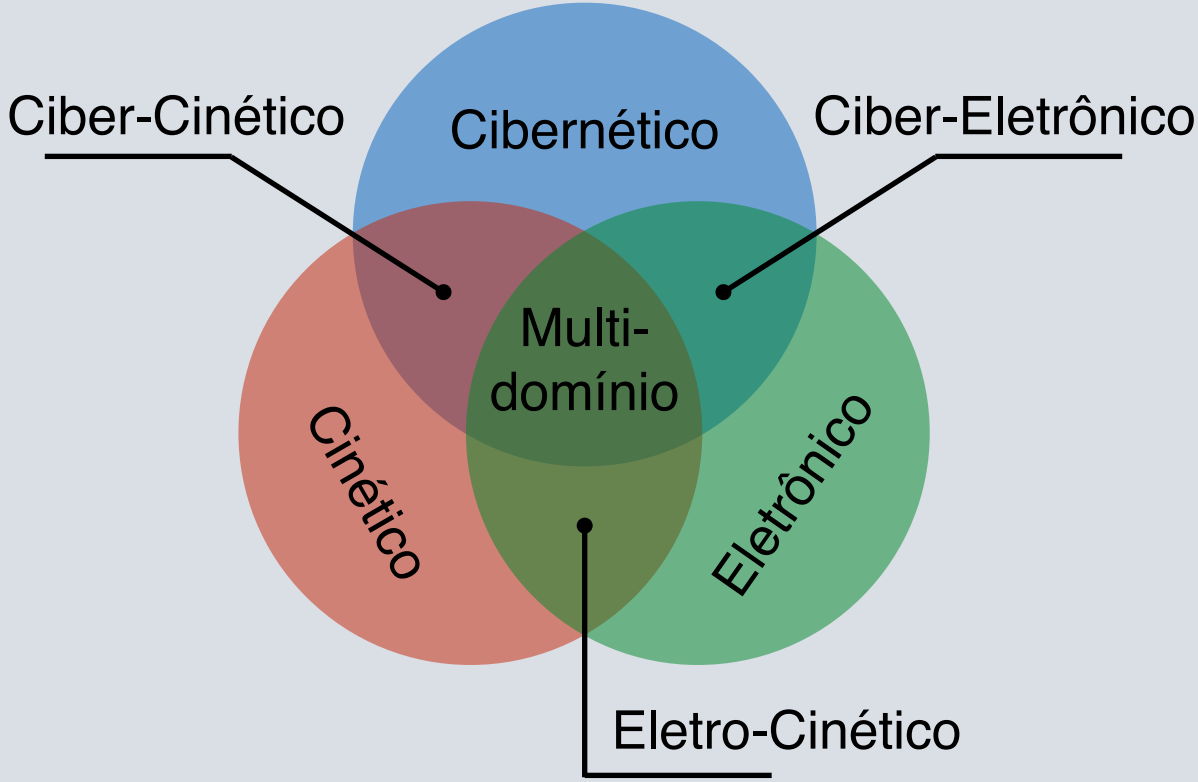
Fonte: DNV GL - Maritime

O Domínio Cibernético no Ambiente Naval

Tecnologia da Informação (TI)
• Administração • Contabilidade • Lista de tripulação • Planejamento de manutenção • Gestão de sobressalentes • Informações de afretamento

Tecnologia Operacional (TO)
• CLPs • SCADA • Instrumentos de medida e controle embarcados • ECDIS • Sistema de controle da propulsão • *Data loggers* • Sistema de controle de carga • Posicionamento dinâmico • *Integrated Navigation System* • etc.

O Domínio Cibernético no Ambiente Naval



Domínio da guerra cinética:

Mundo real – i.e. não virtual – sujeito a mudanças mediante a aplicação de forças.

Domínio da guerra eletrônica:

Espectro eletromagnético – faixas de frequência em que operam sensores, e sistemas de comunicação por ondas eletromagnéticas.

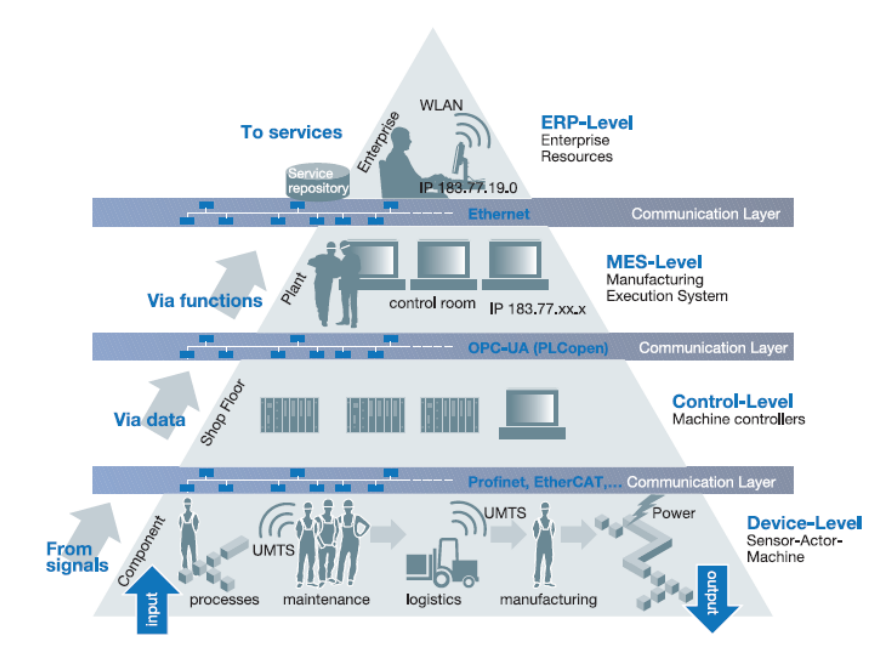
[9] DE SÁ, Alan Oliveira; MACHADO, Raphael Carlos Santos; ALMEIDA, Nival Nunes. **O Encontro da Guerra Cibernética com as Guerras Eletrônica e Cinética no Âmbito do Poder Marítimo**. Revista da Escola de Guerra Naval, v. 25, n. 1, 2019.

Ameaças Digitais no Ambiente Naval

Ameaças Digitais no Ambiente Naval

Ataques ciber-cinéticos:

Ofensivas originadas no domínio cibernético, com o objetivo de causar impactos diretos no domínio cinético.



Exemplos de Alvo:

Sistemas de propulsão de navios (Hart, 2004);

Sistemas de armas (Janer e Proum, 2014);

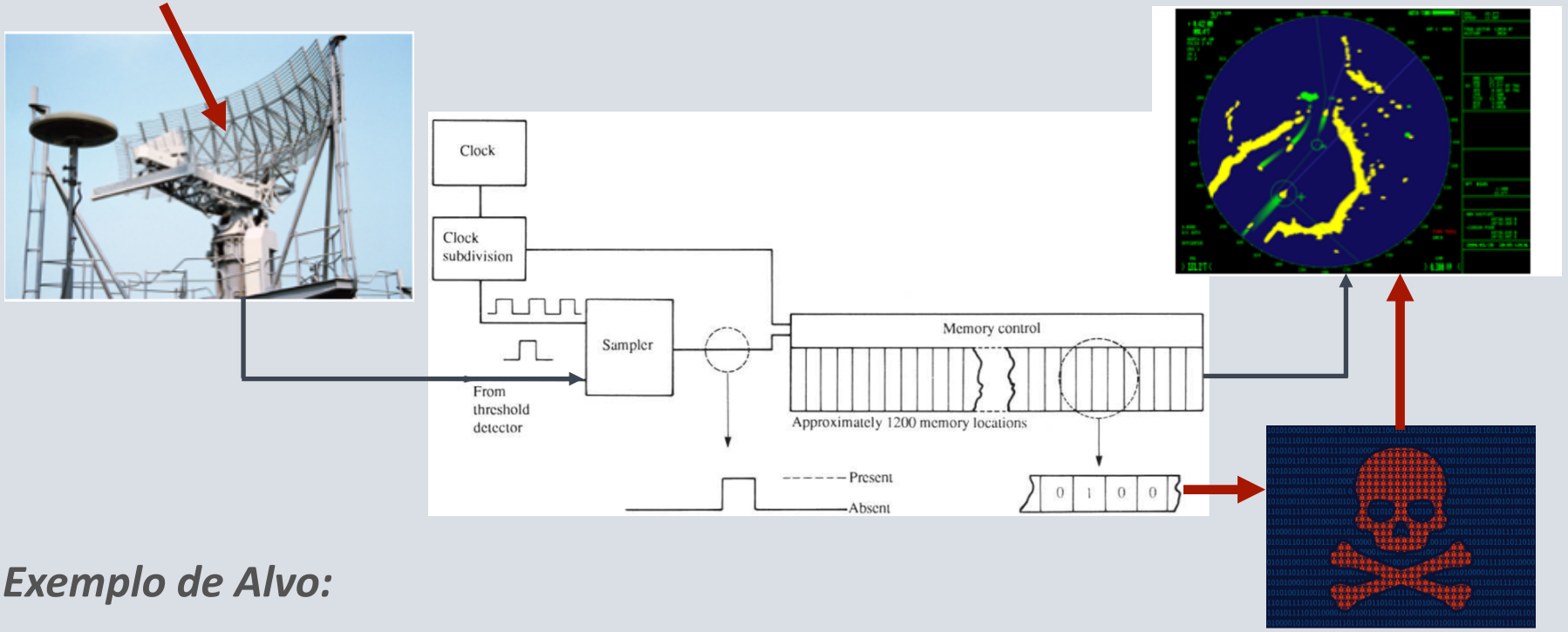
Sistemas offshore de exploração petróleo (Wadhawan e Neuman, 2015);

Ameaças Digitais no Ambiente Naval

Ataques ciber-eletrônicos:

Porta de entrada para comandos: os mesmos dispositivos de captação de ondas eletromagnéticas que o sistema alvo usa para cumprir sua função tática/operacional.

MAE



Exemplo de Alvo:

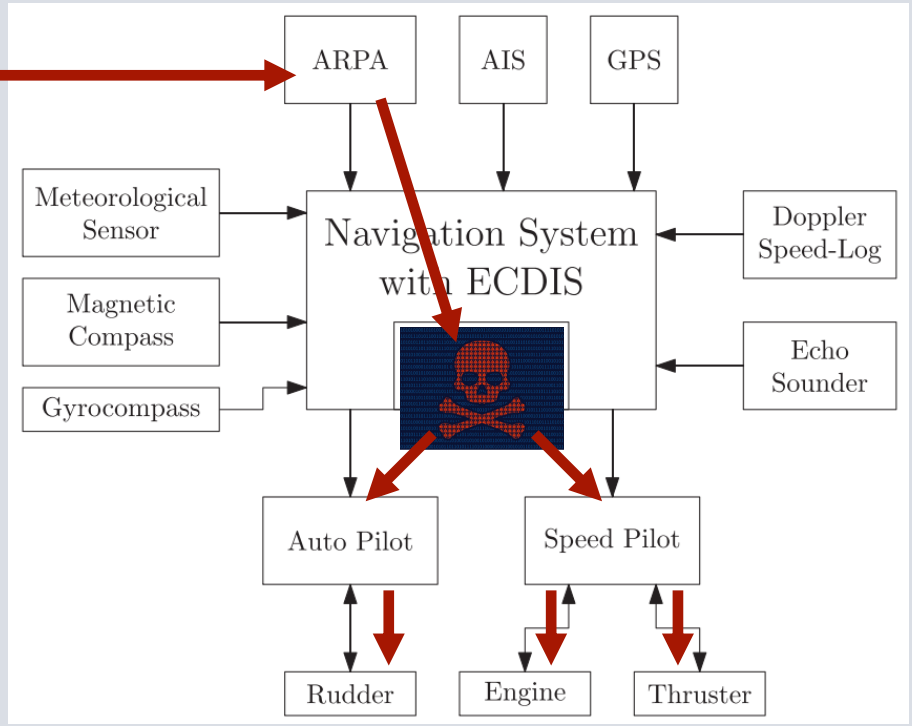
Radar de vídeo digitalizado (Leite Junior; de Sá, 2020)
Integrated Navigation System (LUND et al., 2018)

Ameaças Digitais no Ambiente Naval

Ataques multidomínio:

Porta de entrada: os mesmos dispositivos de captação de ondas eletromagnéticas que o sistema alvo usa para cumprir sua função tática/operacional.

MAE



Componente cibernética: pivô entre domínios da guerras eletrônica e cinética.

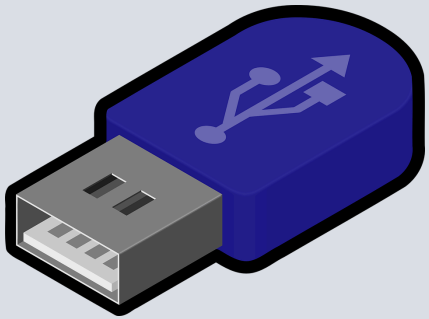
Exemplos de Alvo:

Integrated Bridge System – IBS (Bhatti e Humphreys 2017)

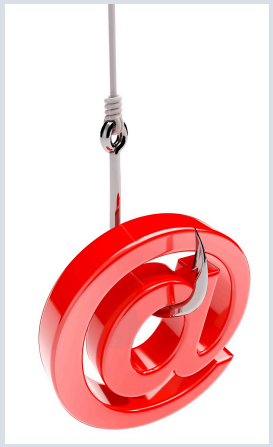
Ameaças Digitais no Ambiente Naval

O embarque das ameaças digitais

Conexões sem fio



Mídias removíveis



Negligência/ desconhecimento

Supply chain attacks

Ameaças Digitais no Ambiente Naval

Tecnologia da Informação (TI)

- Administração
- Contabilidade
- Lista de tripulação
- Planejamento de manutenção
- Gestão de sobressalentes
- Informações de afretamento

Tecnologia Operacional (TO)

- CLPs
- SCADA
- Instrumentos de medida e controle embarcados
- ECDIS
- Sistema de controle da propulsão
- *Data loggers*
- Sistema de controle de carga
- Posicionamento dinâmico
- *Integrated Navigation System*
- etc.

Riscos:

- Financeiros
- Reputação

Riscos:

- Morte
- Instalações e equipamentos
- Ambientais

Conclusões

Conclusões

- Sistemas marítimos estão seguindo as tendências mundiais:
  Indústria 4.0, IoT, *smart sensors*, etc.

- Ataques cibernéticos podem ter **interação com outros domínios** (eletrônico e cinético)

- Embarque de ameaças:
  redes sem fio, mídias removíveis, pessoal, *supply chain attacks*

- Casos ocorridos reforçam a necessidade **pesquisas** e **soluções** para segurança cibernética no setor naval

Perguntas?

Obrigado!

Divulgação

HOME > SPECIAL SESSION #1

Special Session #1

CYBERSECURITY TECHNOLOGIES AND INSTRUMENTS FOR NAVAL SENSORS AND SYSTEMS (NAVALCYBERSEC)

http://www.metrosea.org/special-session-1

O Domínio Cibernético no Ambiente Naval

Perfil dos
Integrated Navigation Systems [9]

Workstations	Multi function 15	ECDIS 5	Unknown 2
Operating system	Windows 11	Linux 1	Unknown 10
Sensor integration	Yes 18	No 3	Unknown 1
Networking	Ethernet 20	CAN-bus 1	Unknown 1
Radar	Networked 13	Direct 3	Unknown 6
ECDIS controlled autopilot	Yes 8		Unknown 14
Internet connection	Yes 12		Unknown 10

1) Astronautics
2) Consilium
3) Furuno
4) iXblue
5) Kongsberg
6) Larsen & Toubro
7) Northrop Gruman Sperry Marine
8) Praxis
9) Rolls-Royce
10) Tokyo Keiki
11) Wärtsilä Valmarine
12) Böning
13) Danelec Marine
14) GEM
15) Kelvin Hughes
16) L3 MAPPS
17) Marine Technologies
18) OSI Maritime Systems
19) Raytheon Anchütz
20) SIMRAD
21) Transas
22) YALTES

[9] LUND, Mass Soldal et al. **Integrity of Integrated Navigation Systems**. In: 2018 IEEE Conference on Communications and Network Security (CNS). IEEE, 2018. p. 1-5.