Departamento de Controle do Espaço Aéreo
IV Centro Integrado de Defesa Aérea e Controle de Tráfego Aéreo

IA Cognitiva aplicada à Segurança Cibernética de Infraestruturas Críticas

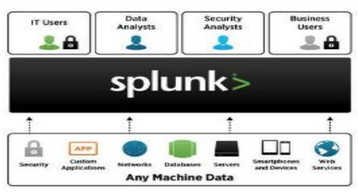
Antônio Henrique Ribeiro Lourenço, Marcelo Mendonça Teixeira,
Marcelo Alexandre Martins da Conceição e Cristiane Domingos de Aquino Teixeira
IV Centro Integrado de Defesa Aérea e Controle de Tráfego Aéreo (CINDACTA IV), Universidade de Pernambuco (UPE),
Instituto Tecnológico de Aeronáutica (ITA) e Universidade Federal Rural de Pernambuco (UFRPE)

Resumo — Na atualidade diversos ataques cibernéticos vêm sendo realizados contra nações, principalmente contra infraestruturas críticas, como estações de energia elétrica, indústrias nucleares e diversas outras. A carência de modelos descritivos para segurança cibernética para infraestruturas críticas, motivou os autores deste pôster a proporem um modelo baseado em Inteligência Cognitiva, para preencher essas lacunas. Dessa forma, o objetivo deste pôster é conceituar e apresentar um modelo inicial e suas premissas para a questão da segurança cibernética para infraestruturas críticas.

I. INTRODUÇÃO

Infraestruturas Críticas (IC) de um país são de fundamental importância para manutenção da segurança nacional, vitalidade econômica, saúde e segurança pública. Ataques cibernéticos em infraestruturas críticas têm objetivos diferentes: razões político-sociais, fins lucrativos, razões geopolíticas ou ciberespionagem de nação para nação. É fato que as vulnerabilidades em evidência em sistemas computacionais na sociedade contemporânea, cada vez mais digital e ávida por desenvolvimento tecnológico, trazem riscos eminentes à estabilidade social e a segurança dos países, interferindo direto e indiretamente na vida de governos, empresas e cidadãos, nunca antes visto. Ou seja, versa uma possibilidade real de estabilidade que sobrepõe às hipóteses de "*Simulacres et Simulation"* [1].

Em justaposição, Assange et al. [2] destacam que a Internet deveria ser um espaço civil, mas se transformou em um espaço militarizado no decorrer dos anos, especialmente com a sua popularização de acesso. Todavia, o conceito de Internet de Bob Kahn e Vint Cerf (desenvolvedores) era disponibilizar para a humanidade um espaço geográfico sem barreiras, livre e democrático [3].



Na prática, à medida que os ataques virtuais crescem em vertiginosamente, surge a necessidade de implementação de uma solução efetiva para prevenir e/ou corrigir as falhas e os impactos ilícitos causados aos sistemas computacionais mencionados em epígrafe, entre as quais se destaca a inteligência artificial (IA). Em adição, versa a segurança cognitiva, combinando as contribuições da Inteligência Artificial com as da inteligência humana, antessala do que conhecemos como *Machine Learning*.

A segurança cognitiva combina os pontos fortes da inteligência artificial com os da inteligência humana. A IA cognitiva aprende com cada interação para detectar e analisar ameaças, de maneira proativa, fornecendo *insights* práticos para analistas de segurança para tomada de decisões informadas, com velocidade e precisão. Aqui, se destaca os objetivos do artigo em voga, tendo como princípio basilar responder as seguintes perguntas de investigação: (1) Quais as perspectivas de segurança da informação diante de artefatos complexos de guerra cibernética, como o Stuxnet, seguido do Duqu e Flame, capazes de destruir projetos estratégicos e de desenvolvimento de uma nação? (2) E, como propor modelos de inteligência artificial (IA) cognitiva, combinando os pontos fortes da IA com os da inteligência humana, com o intuito e desafio de proteção de infraestruturas críticas, contra diversas ameaças cibernéticas sofisticadas e ameaçadoras?

II. METODOLOGIA

A trajetória metodológica do presente trabalho, de abordagem qualitativo, baseia-se em um estudo exploratório e empírico-descritivo. Ao nível dos métodos e técnicas, recorremos a Revisão de Literatura, ao Estudo de Caso e à Análise de Requisitos (funcionais e não funcionais). Enquanto método, a revisão de literatura deve conter informações atuais sobre a problemática a ser estudada, razão pela qual se torna essencial para o pesquisador que se inicia na pesquisa científica, porque o auxilia a definir com precisão o objeto de sua investigação, bem como lhe mostra se a pesquisa que realiza pode trazer uma contribuição adicional sobre o tema para o conhecimento, afirma Coutinho [4].

III. MODELO PROPOSTO – IAC 1.0

Os recursos do modelo de Segurança Cognitiva (IAc 1.0) são centrados no conjunto de premissas descritas a seguir, agrupadas em conjuntos, proporcionando o nível de segurança adequado para aplicação eficaz em infraestruturas críticas. Dessa forma, proporcionado visibilidade adequada, controle e resposta a ameaças cibernéticas complexas de forma automatizada.
Com a intenção de tornar o modelo mais eficaz, os gerentes/administradores de rede necessitam realizar adequações ambientais prévias, conhecendo fragilidades e as tratando previamente, adotando as melhores práticas e seguindo as Normas e Referências a seguir. **ISO 27001** é uma norma padrão e de referência Internacional para a gestão de segurança da informação. **IEC62443** é uma norma de Segurança Cibernética para Sistemas de Automação. **CISA** fornece amplo conhecimento e práticas de segurança cibernética à infraestruturas criticas. **NIST SP. 800-82r2** é um dos laboratórios mais antigos de pesquisa em ciências tecnológicas. **CIS** - O Centro de controles críticos de segurança da Internet para uma defesa cibernética eficaz é uma publicação de diretrizes de práticas recomendadas para segurança de computadores. Sua missão é identificar, desenvolver, validar, promover e manter soluções de melhores práticas para defesa cibernética e criar e liderar comunidades para permitir um ambiente de confiança em ciberespaço.

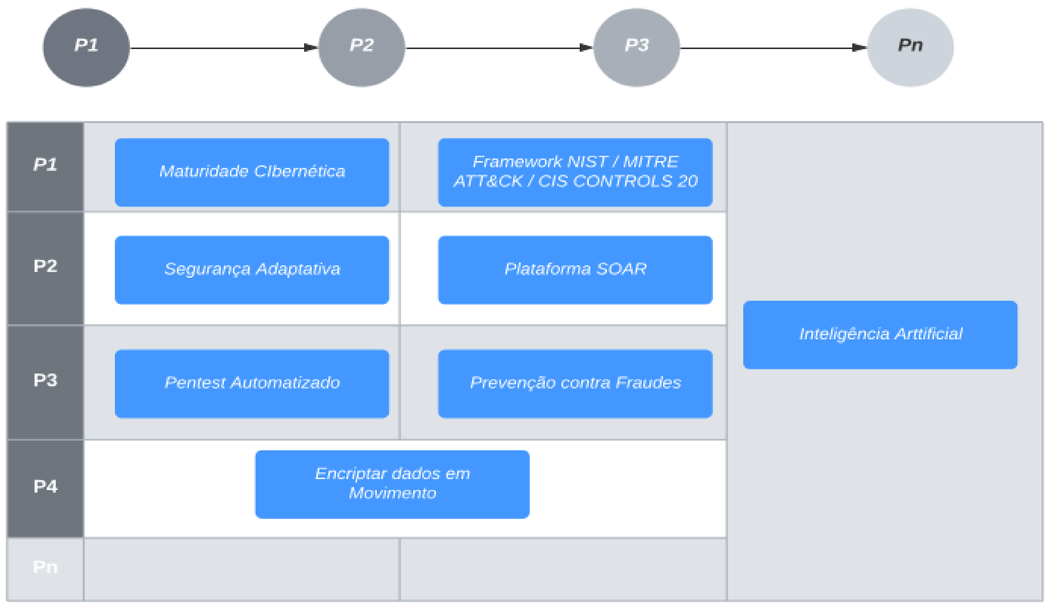


Figura 1 – Modelo IAc 1.0.

Para que seja possível implantar o modelo, devem ser levadas em consideração as seguintes premissas: **Conheça sua rede**: visualize, modele e projete uma rede *zero trust* (zero confiança), onde todas as camadas são checadas em tempo real; **Segregação Física e Lógica**: isole ativos, independentemente do ambiente, rede ou dispositivo; **Proteja Ativos Críticos**: proteja servidores físicos, máquinas virtuais, dispositivos de uso específico com Controle de Acesso e Configuração restrito, sendo periodicamente revisado, isolado da Internet, não sendo admitido mídias do tipo (CD, DVD, Pen Drive, entre outros); **Gestão de Ativos**: gerencie automatizada, minuciosa e detalhadamente ativos de hardware e software da organização; **Gestão de *Logs***: implante soluções SIEM; **Política de Segurança**: defina suas Política de Segurança da Informação e em operação na Organização; **Controle de Sistemas Legados**: mantenha-os segregados da rede, sem conectividade com a Internet; **Controle dos Riscos e Vulnerabilidades**: controle periodicamente riscos e vulnerabilidades; e **Plano de Capacitação e Conscientização dos Colaboradores**: capacite profissionais de TI, por meio de treinamentos, cursos, certificações, e palestras de conscientização para os membros da corporação.

Etapas do Modelo IAc 1.0: **Maturidade Cibernética**: classificar, diagnosticar e exibir a maturidade cibernética do ambiente. A plataforma de orquestração, automação e resposta de segurança mais abrangente do setor com gerenciamento nativo de inteligência contra ameaças e um mercado integrado; **Plataforma SOAR**: implantar a plataforma de orquestração, automação e resposta de segurança abrangente e integrada com gerenciamento nativo de inteligência contra ameaças nos ambientes de *Network Operations Center* (NOC) e *Security Operations Center* (SOC); **CIS Controls 20**: aplicar os 20 controles críticos de segurança recomendados pelo CIS; **NIST CSF**: implementar o framework NIST; **Inteligência Artificial**: é usado onde temos uma grande quantidade de dados de treino mas apenas alguns são supervisionados. É possível usar esse tipo de algoritmo quando você quer o algoritmo aprenda informações nos dados mas também aprenda usando alguns dados supervisionados; **Pentest Automatizado**: identificar e corrigir vulnerabilidades; **Segurança Adaptativa**: integrar ferramentas de segurança existentes para correlação, detecção e resposta a ameaças; **Encriptar dados em movimento**: impedir a detecção/alteração de pacotes; e **Prevenção contra Fraudes**: verificar identidades com biometria física e comportamental, além de implementar autenticação multifatorial.

IV. CONCLUSÃO

O O presente pôster apresenta brevemente um modelo inicial para segurança cibernética, com base em inteligência artificial para automação e orquestração de processos. Os recursos do modelo de segurança cognitiva são centrados no conjunto de premissas propostas, agrupadas em conjuntos, de forma a proporcionar o nível de segurança adequado para aplicação eficaz em infraestruturas críticas de um país, proporcionando visibilidade adequada, controle e resposta a ameaças cibernéticas complexas de forma automatizada As premissas e restrições, para eficácia do modelo proposto, foram brevemente descritas e embasadas por meio das principais normas, referências e frameworks de cibersegurança. Como direcionamento para trabalhos futuros e por se tratar de um estudo inicial, os autores deste pôster sugerem aplicar o modelo proposto a estudos de caso, validando os resultados obtidos e os comparando com resultados obtidos pela literatura. Também, deverão ser investigadas as diferentes técnicas de inteligência cognitiva, que possam agregar valor na implantação do modelo. Dessa forma, as questões de pesquisa descritas poderão ser respondidas.

REFERÊNCIAS

[1] J. Baudrillard, "Simulacres et Simulation", Paris, Galilée, 1981.
[2] J. Assange, J. Appelbaum, A. Müller-Maguhn, J. Zimmermann. Cypherpunks: Freedom and the Future of the Internet, NewYork, 2012.
[3] M. Teixeira, R. Do Nascimento, C. de Aquino, As *Fake News* No Letramento Digital: Da Propaganda Enganosa à Leitura Crítica das Mídias: Um Estudo Empírico Descritivo. GRIN Verlag, 2018.
[4] C. P. Coutinho, Metodologia de investigação em ciências sociais e humanas. Leya, 2014.