Atuação colaborativa da Defesa Cibernética na proteção de infraestruturas críticas de interesse para a Defesa Nacional

Ten Cel Com Walbery Nogueira de Lima e Silva*

RESUMO

O horizonte cibernético da próxima década tende a ampliar a conexão global, trazendo mais usuários para este domínio e ofertando novas tecnologias, tais como redes 5G e inteligência artificial. As ameaças poderão empregar o espaço cibernético para ações que geram efeitos cinéticos e não cinéticos sobre infraestruturas críticas (IEC) de interesse para a Defesa Nacional, com o risco de provocar paralisia estratégica no funcionamento de países, conforme já ocorreu nos ataques à Estônia (2007) e à Ucrânia (2014). As Forças Armadas estão diretamente ligadas a este tema, uma vez que dependem de produtos e serviços do setor privado para manterem a operacionalidade e, no caso de grave crise, poderão ter tropas empregadas no contexto da Defesa Nacional. Este artigo levanta a importância da atuação colaborativa envolvendo governo, defesa, academia e setor privado, aliada à cooperação internacional, como forma de incrementar a resiliência cibernética. É apresentada a experiência do Comando de Defesa Cibernética na condução do exercício interagências Guardião Cibernético (EGC). A atividade simulada, ocorrida em julho de 2019, contou com a participação de empresas e organizações dos setores elétrico, financeiro, nuclear e de telecomunicações, bem como de observadores internacionais do Cooperative Cyber Defence Center of Excelence da OTAN e de nações amigas. O EGC permitiu praticar processos de tomada de decisão e procedimentos técnicos. Neste artigo são evidenciados a concepção do exercício, os ensinamentos colhidos para a proteção de IEC e a evolução do EGC que na 3ª edição terá cenário cibernético contendo desafios da próxima década e a inclusão dos setores de transporte aéreo e de fornecimento de água.

Palavras-chave: Espaço cibernético. Atuação colaborativa. Infraestruturas críticas.

Collaborative approach of Cyber Defense to protect critical infrastructure of interest for National Defense

ABSTRACT

The cyber horizon of the next decade tends to broaden the global connection, bringing more users into this domain and expanding new technologies such as 5G networks and artificial intelligence. Threats can use cyberspace for actions that result in kinetic effects and non-kinectic effects on National Defense critical infrastructure (CI) with the risk of causing strategic paralysis in the countries, as occurred in the attacks on Estonia (2007) and Ukraine (2014). The Armed Forces are directly tied to this issue because they rely on private sector products and services to maintain their operationality and in case of an incident with severe crisis troops may be deployed. This essay moots the importance of collaborative approach involving government, defense, academia and the industry, integrated with international cooperation in a unity of effort to enhance cyber resilience. It is presented the interagency exercise Cyber Guardian (CG) study case that is coordinated by the Brazilian Cyber Defense Command. The second edition of this drill, which took place in July 2019, was attended by companies and organizations from the electrical, financial, nuclear and telecommunications sectors as well as international observers from NATO Cooperative Cyber Defense Center of Excellence and partner nations. The CG aims to practice decision-making processes and technical procedures. This article presents the exercise specification, lessons learned to increase critical infrastructure protection and CG evolution that in 3rd edition will have incident scenarios regarding cyber challenges for the next decade as well as the addition of air transport and water supply sectors.

Keywords: *Cyberspace. Collaborative approach. Critical infrastructure.*

Artigo recebido em 01/12/2019 e aceito para publicação em 1/01/2020

1 INTRODUÇÃO

A próxima década sinaliza a adoção de novos recursos que serão disponibilizados para o funcionamento da sociedade moderna cada vez mais dependente de tecnologias que serão usadas para potencializar a capacidade de operação das infraestruturas críticas (IEC) e para elevar a um novo patamar a variedade de serviços ao usuário final no mundo interconectado (NATO, 2019).

Ao mesmo tempo, as ameaças cibernéticas tendem a continuar explorando vulnerabilidades para fins diversos, tais como espionagem, hacktivismo, terrorismo e ações perpetradas por estados nação, o que pode conduzir a cenários catastróficos de paralisia estratégica de países. A história recente revela exemplos disso, conforme ataques cibernéticos de grande impacto nacional ocorridos na Estônia em 2007 e na Ucrânia em 2014 (E-ISAC, 2016).

Ressalta-se que as Forças Armadas (FA) têm uma ligação direta com este tema, uma vez que é cliente de muitos serviços e produtos oriundos da indústria para ter sua plena capacidade operativa, bem como poderá ser acionada para restabelecer a lei e a ordem no caso de ataque cibernético de grande envergadura que comprometa a segurança interna, conforme prevê o Sistema Militar de Defesa Cibernética (Ministério da Defesa, 2014).

Em meio a esse ambiente interconectado, de ações no mundo virtual que podem gerar efeitos cinéticos, a atuação colaborativa envolvendo governo, defesa, academia e setor privado, aliada à cooperação internacional, mostra-se como um caminho desejável para garantir a unidade de esforço necessária ao incremento da resiliência cibernética. Quais ações podem ser feitas nesse sentido? Qual seria o papel das FA em situação de guerra e de não-guerra?

Este artigo levanta a importância da atuação integrada em ambiente interagências, apresentando como estudo de caso o Exercício Guardião Cibernético (EGC), o qual é conduzido anualmente pelo Comando de Defesa Cibernética (ComDCiber) e é voltado para a proteção de infraestruturas críticas (IEC) de interesse para a Defesa Nacional.

A 2ª edição do EGC foi realizada no período de 02 a 04 de julho de 2019, nas instalações do ComDCiber e do Centro de Instrução de Guerra Eletrônica (CIGE), contando com a participação de 215 representantes de 41 empresas e organizações.

O exercício está alinhado com a Política Nacional de Segurança da Informação (PNSI) e com a Estratégia Nacional de Segurança Cibernética (E-Ciber) do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), as quais preveem a elevação do nível de proteção do governo e das infraestruturas críticas por meio de ações baseadas na cooperação.

2 DESENVOLVIMENTO

2.1 CONCEPÇÃO DO EGC 2.0

O EGC 2.0 teve por finalidade contribuir para o incremento do nível de proteção do espaço cibernético nas infraestruturas críticas de interesse para a Defesa Nacional nos seguintes setores: elétrico, financeiro, nuclear e telecomunicações.

Para o cumprimento do seu propósito, foram estabelecidos os seguintes objetivos:

a) coordenar e integrar, em ambiente interagências, a segurança e defesa cibernéticas para a proteção de infraestruturas críticas;

b) exercitar o processo decisório em diferentes níveis de responsabilidade e de competência, incentivando a atuação colaborativa na prevenção, solução e mitigação de danos causados por ameaças existentes no espaço cibernético;

c) verificar a efetividade de procedimentos para a solução de incidentes em infraestruturas críticas;

d) contribuir para a integração do governo, defesa, comunidade acadêmica e setor privado, por meio de simulações virtual e construtiva, bem como propondo contribuição de normativas;

e) aplicar boas práticas de proteção cibernética nas ações preventivas e reativas frente a incidentes cibernéticos;

f) empregar ferramentas para o compartilhamento de informação; e

g) proporcionar ambiente favorável para que as empresas e organizações simulem incidentes que permitam colher ensinamentos para o aprimoramento de processos e protocolos internos.

O exercício contou com a participação de representantes de diversas áreas de interesse para o ecossistema cibernético, conforme descrito a seguir:

Quadro 1— Participantes do EGC 2.0

Área Estratégica	Participantes
Defesa	Chefia de Operações Conjuntas (CHOC), Assessoria de Doutrina e Legislação (ADL), Comissão Interescolar de Doutrina de Operações Conjuntas (CIDOC), Diretoria de Comunicações e de Tecnologia da Informação da Marinha (DCTIM), CTIM, CITEx, Comando de Comunicações e de Guerra Eletrônica do Exército (Cmdo Com GE Ex), Departamento de Controle do Espaço Aéreo (DECEA) e Centro de Computação da Aeronáutica em Brasília (CCA BR).
Setor Elétrico	Operador Nacional do Sistema Elétrico (ONS), Agência Nacional de Energia Elétrica, Itaipu Binacional, Companhia de Transmissão de Energia Elétrica Paulista e Furnas.
Setor Financeiro	Banco Central (Bacen), Federação Brasileira de Bancos, Banco do Brasil, Caixa Econômica Federal, Banco Bradesco, Banco Itaú, Banco Santander, B3 Infraestrutura de mercado financeiro, Comissão de Valores Mobiliários e Câmara Interbancária de Pagamentos.
Setor Nuclear	Departamento de Coordenação do Sistema de Proteção ao Programa Nuclear Brasileiro (DCSIPRON-GSI/PR), Comissão Nacional de Energia Nuclear, Indústrias Nucleares Brasileiras, Eletrobras, Eletronuclear, Instituto de Pesquisas Energéticas e Nucleares, Centro Tecnológico da Marinha em São Paulo, Agência Internacional de Energia Atômica e Universidade de São Paulo.
Setor de Telecomunicações	Agência Nacional de Telecomunicações (Anatel), CLARO, OI, Telebras, Telefônica e TIM.
Órgãos Parceiros	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, Centro de Tratamento de Incidentes de Rede do Governo, Agência Brasileira de Inteligência, Divisão de Tecnologias Sensíveis do Ministério das Relações Exteriores, Serviço de Repressão a Crimes Cibernéticos do Departamento da Polícia Federal, Serviço Federal de Processamento de Dados e Rede Nacional de Ensino e Pesquisa.
Comunidade Acadêmica	Escola Superior de Guerra, Universidade de Campinas e Universidade de São Paulo.
Observadores Internacionais	Agência Internacional de Energia Atômica (AIEA), Centro Cooperativo de Excelência em Defesa Cibernética da OTAN (CCDCOE), empresa SAAB de desenvolvimento do projeto FX-2 Gripen, bem como adidos e representantes dos Estados Unidos da América, Portugal, Suécia e Tailândia .

Fonte: o autor, 2019.

2.2 ESTRUTURA DE SIMULAÇÃO

O exercício adotou técnicas de simulação virtual e construtiva de forma integrada.

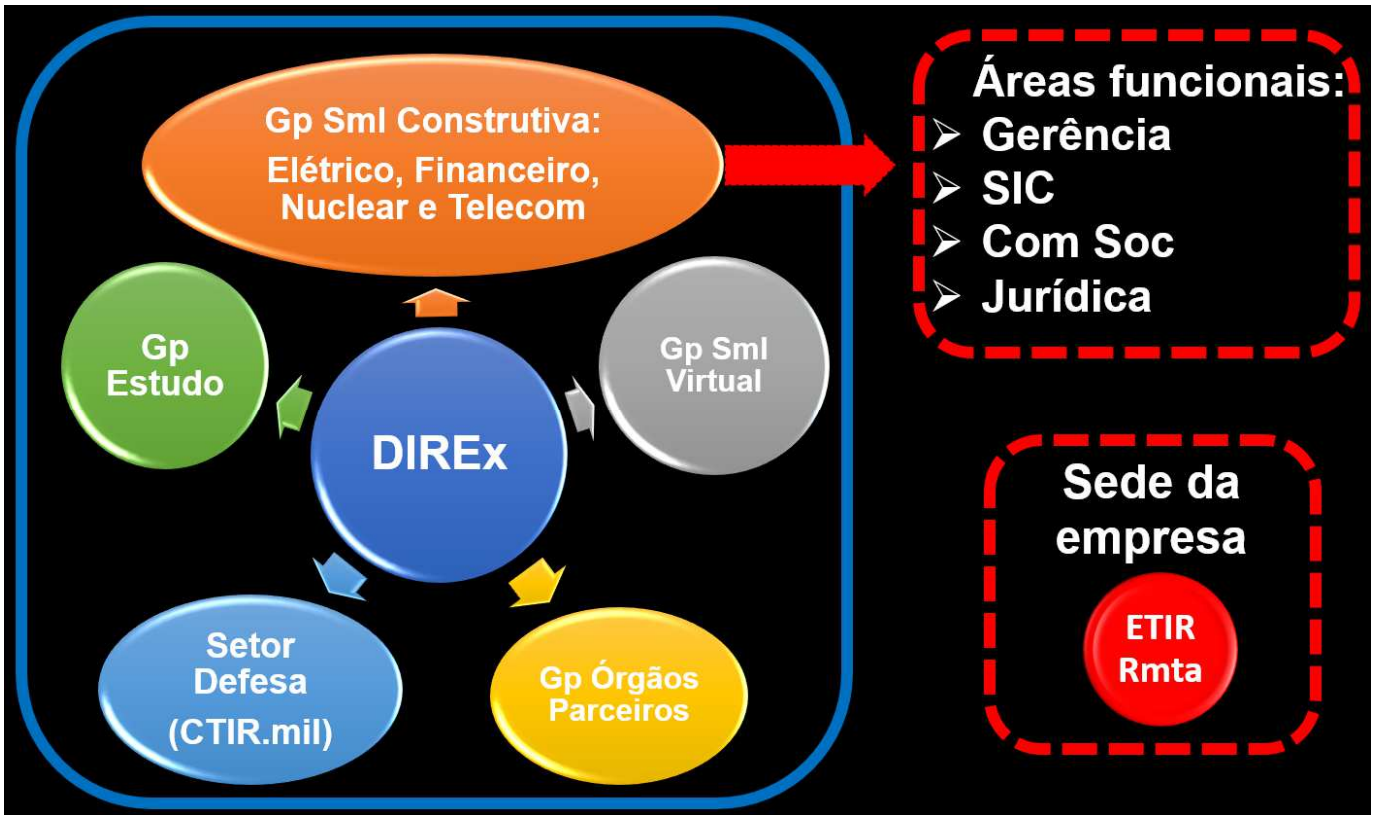
A simulação virtual teve o objetivo de identificar e difundir as melhores práticas das equipes de tratamento de incidentes de rede. A simulação construtiva permitiu exercitar o nível gerencial das organizações participantes na solução de problemas cibernéticos, por meio de ações envolvendo as áreas de segurança da informação, departamento jurídico e comunicação social.

Para envio e resposta dos problemas simulados a Direção do Exercício (DIREx) empregou como ferramenta o sistema de acompanhamento de eventos denominado *Request Tracker* (RT), o qual foi customizado pelo ComDCiber para uso no EGC 2.0.

A elaboração dos problemas simulados foi coordenada pelo Estado-Maior Conjunto (EM Cj) do ComDCiber em estreita ligação com as entidades centrais das organizações participantes nas diferentes áreas: Operador Nacional do Sistema Elétrico, Banco Central do Brasil, Departamento de Coordenação do Sistema de Proteção ao Programa Nuclear Brasileiro e Anatel.

Os representantes da Defesa Cibernética das Forças Armadas constituíram uma equipe conjunta para tratamento de incidentes de rede com atuação colaborativa do Centro de Tecnologia da Informação da Marinha, do Centro Integrado de Telemática do Exército e do Centro de Computação da Aeronáutica de Brasília.

Figura 1—Estrutura do EGC 2.0



Fonte: o autor (2019).

Empregou-se um cenário fictício de não-guerra, envolvendo as Forças Armadas e as áreas estratégicas de interesse para a Defesa Nacional.

Durante a execução do EGC 2.0 os incidentes foram apresentados de modo gradativo e intersetores, inclusive com o estabelecimento de um "Gabinete Nacional de Segurança Cibernética", para gerenciar as ações de Estado no ápice da crise do ambiente hipotético de conflito apresentado.

Os eventos simulados para os gabinetes de crise foram preparados durante o ciclo de planejamento, de modo conjunto e integrado com todos os envolvidos.

Para a elaboração dos eventos cibernéticos foram elencados temas nos quais poderiam ser desenvolvidas a interação intraempresa, intrasetor e intersetores.

A fim de facilitar a descrição dos eventos para o *table-top*, cada desafio proposto foi detalhado com base na resposta aos seguintes aspectos: o que, quando, quem, onde, por que, como e prejuízo gerado (5W2H). Foram preparadas soluções possíveis contendo: medidas reativas, medidas preventivas, bem como a interação entre os setores e organizações.

A seguir são descritas as principais áreas temáticas dos eventos simulados:

a) setor elétrico: estações de trabalho criptografadas por ransomware, envio de comandos indevidos para instalações, indisponibilidade de servidores Supervisory Control and Data Acquisition (SCADA), via ataques às instalações por distributed denial-of-service (DDoS), informações incorretas apresentadas nas consoles das salas de controle, engenharia social, indisponibilidade de redes de telecomunicações e vazamento de dados pessoais;

b) setor financeiro: indisponibilidade de estações e servidores Windows; transferências fraudulentas nos sistemas de pagamento interbancários; comprometimento da integridade dos sistemas de pagamento; e extorsão por vazamento de dados;

c) setor nuclear: ataque a instalações do ciclo de enriquecimento de combustível; vazamento de informações sensíveis; bem como comprometimento do sistema SCADA e de programmable logic controller (PLC);e

d) setor de telecomunicações: ataque do tipo Border Gateway Protocol (BGP).

Os cenários foram integrados de modo a permitir o uso da minuta do Plano Nacional de Tratamento de Incidentes de Redes, a fim de colher impressões para a sua posterior validação por parte do GSI/PR.

2.3 EMPREGO DO MALWARE INFORMATION SHARING PLATFORM (MISP)

Fruto de parceria com o Centro de Defesa Cibernética de Portugal, o ComDCiber está em fase de testes do MISP, ferramenta voltada para a troca de informações online sobre artefatos maliciosos amplamente utilizada pelos países da Organização do Tratado do Atlântico Norte (NATO, 2019).

O MISP é baseado em plataforma web, consistindo de uma comunidade voltada para o compartilhamento confiável de informações técnicas sobre malware com diferentes níveis de Traffic Light Protocol.

Trata-se da combinação multidirecional de repositórios com mecanismos para inserção e busca de dados. Permite a integração com Application Programming Interface (API) para produção de conhecimento e consciência situacional.

Uma de suas grandes vantagens é a rapidez com que permite registrar informações e contramedidas que podem ser adotadas para evitar que uma ameaça cibernética se propague.

Durante o EGC foram disponibilizadas contas de acesso à instância MISP do ComDCiber a todas as empresas e organizações participantes, o que permitiu apresentar a ferramenta e praticar o seu uso no âmbito das IEC.

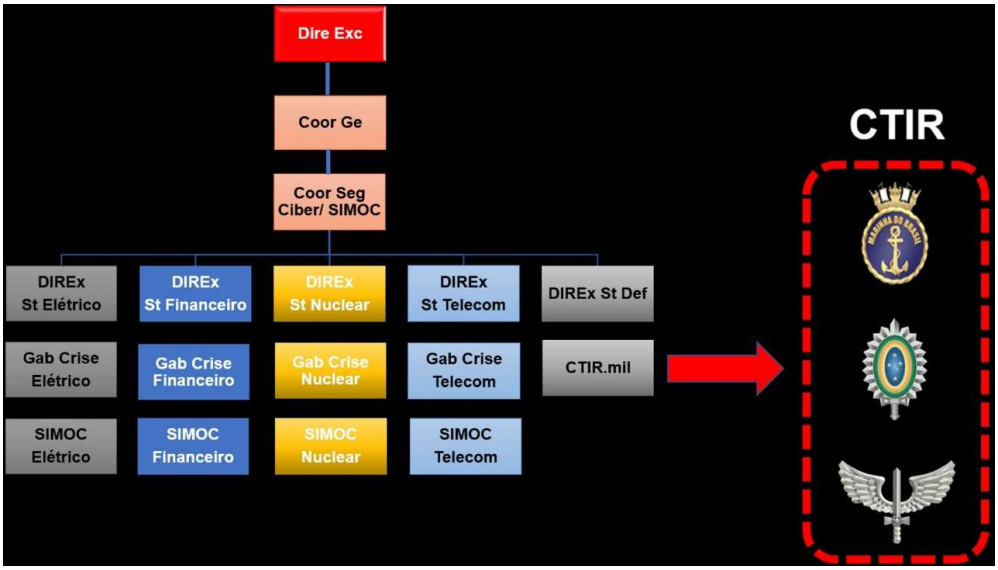
2.4 CONDUÇÃO DO EXERCÍCIO

A coordenação do EGC 2.0 foi realizada pelo ComDCiber em estreita ligação com os órgãos parceiros e empresas participantes.

A fim de facilitar os trabalhos, os órgãos centrais de cada área estratégica tiveram o encargo de capilarizar o planejamento, preparação e verificação das respostas aos incidentes simulados (Bacen, Anatel, DCSIPRON e ONS).

Foi adotada a seguinte organização das células de trabalho:

Figura 2—Estrutura do ECG 2.0



Fonte: o autor (2019).

2.4.1 Direção do exercício

Composta por integrantes de ComDCiber, CTIM, CITEx, CCA-BR, Cmdo Com GE Ex, bem como por 1(um) representante oriundo de cada empresa e organização participante.

2.4.2 Gabinetes de Crise – simulação construtiva (table-top exercise)

Células onde atuaram os participantes de nível gerencial das áreas estratégicas.

Cada empresa e organização participou com 1 (um) profissional oriundo de cada uma das seguintes áreas: gerência de segurança da informação, alta administração, comunicação social e assessoria jurídica.

Os problemas simulados gerados pela DIREx foram encaminhados para os gabinetes de crise por intermédio da ferramenta Request Tracker. Ao receberem os eventos as equipes tinham que apresentar as medidas reativas e preventivas, bem como a interação com as demais áreas estratégicas e órgãos parceiros, concluindo com a indicação de ensinamentos colhidos.

2.4.3 Grupo Órgãos Parceiros

Interagiram de modo colaborativo com as áreas estratégicas para a solução dos problemas simulados.

2.4.4 Grupo de Simulação Virtual

Foram empregados o Simulador de Operações Cibernéticas (SIMOC) e o Simulador de Planta Nuclear (SPN) para emulação de redes computacionais, a fim de identificar e corrigir vulnerabilidades.

Ressalta-se que a equipe do CIGE contou com o apoio de técnicos do SERPRO para a criação de cenários cibernéticos no SIMOC.

Cada empresa e organização convidada participou com 1 (um) especialista de nível técnico operando os cyber ranges citados.

O SPN em sua versão inicial foi desenvolvido pelo CTMSP em parceria com a AIEA e foi empregado pela primeira vez durante o EGC. Contou com a presença de observador internacional oriundo da referida agência e permitiu avaliar o impacto de ataques cibernéticos sobre instalação nuclear.

2.4.5 Grupo Defesa

Atuou de forma conjunta e integrada, constituindo um Centro de Tratamento de Incidentes de Redes Militar.

Respondeu a eventos que tiveram origem sobre as IEC e que geraram efeitos sobre o nível de operacionalidade das Forças. Como exemplos:

a) ataque cibernético sobre data center em provedor de telecomunicações afetou a velocidade de conexão das infovias, degradando a operação do Sistema de Monitoramento de Fronteiras;

b) ramsonware em redes computacionais do sistema financeiro impediu que a Defesa emitisse ordens bancárias para o pagamento de prestadoras de serviços, prejudicando a manutenção do material de emprego militar;

c) instabilidade no sistema SCADA de controle das linhas de transmissão prejudicou o fornecimento de energia elétrica a organizações militares estratégicas para a Defesa Nacional.

2.5 WORKSHOP SOBRE GESTÃO DE RISCO CIBERNÉTICO

Durante a fase de preparação do EGC, na Reunião Final de Coodenação, foi realizado o 1º Workshop em Gestão de Riscos Cibernéticos, contando com a presença de especialistas norte-americanos do *National Institute of Standards and Technology* (NIST).

Estes *experts* apresentaram o *Cybersecurity Framework* e participaram dos estudos nas salas temáticas dos setores elétrico, financeiro, nuclear e de telecomunicações abordando os seguintes temas:

a) gestão de Riscos da Segurança Cibernética das Infraestruturas Críticas;

b) indicadores e pontos de controle para as IEC que podem ser utilizados por órgãos de governo;

c) estrutura para processos de identificação dos ativos que, se atacados, geram maior impacto;

d) análise de riscos e proposição de planos de ação para cada setor estratégico;

e) privacidade de dados e liberdade civil;

f) *benchmarking* de programas de gerenciamento de riscos cibernéticos implementados pelas empresas;e

g) como aplicar o Framework do NIST nos diferentes setores estratégicos e principais dificuldades para implementação.

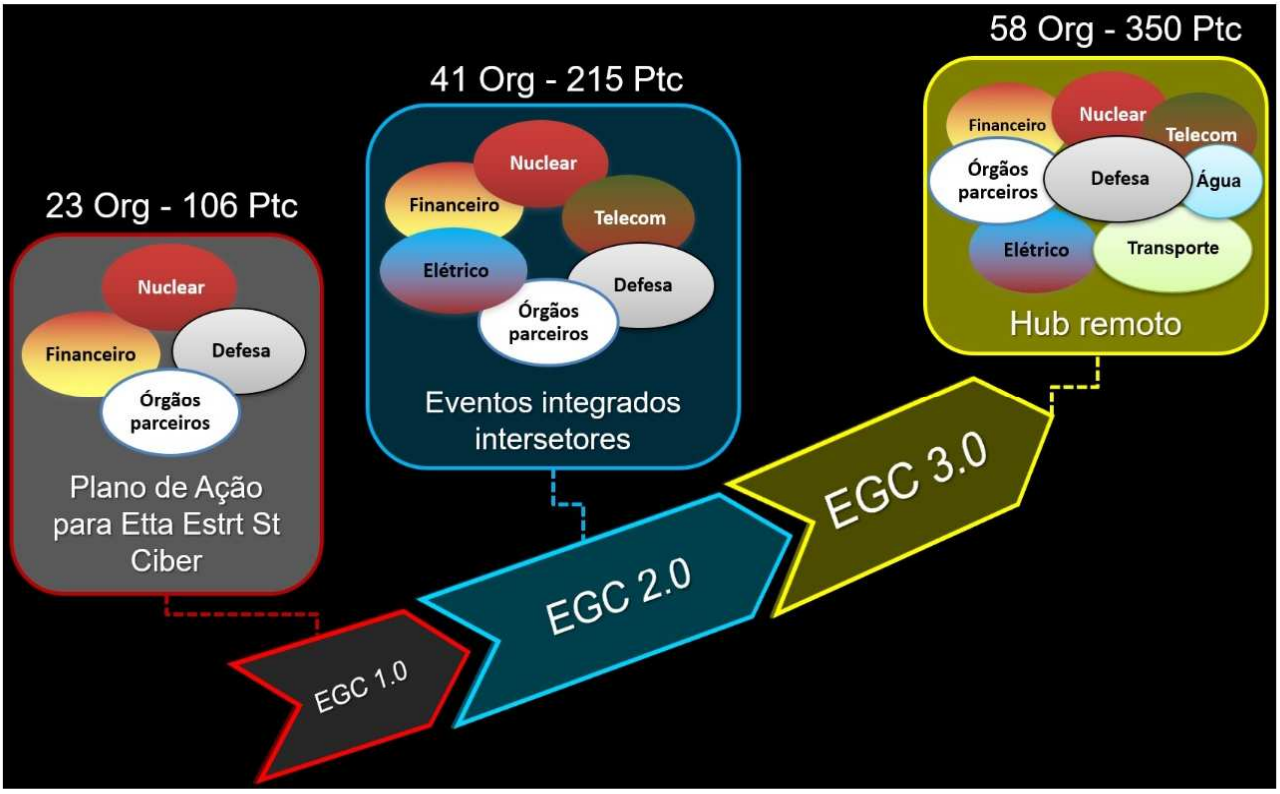
2.6 EVOLUÇÃO DO EGC PARA a 3ª EDIÇÃO

Quadro 2 - Principais aspectos de evolução do ECG 3.0

Linha de Esforço	Evolução
Simulações Virtual e Construtiva	Inserção dos setores de Água e Transporte Aéreo nas simulações virtual e construtiva
	Prática de incidentes relacionados aos "Desafios da Próxima Década", envolvendo inteligência artificial, telefonia móvel 5G e ataques a redes de cabos submarinos
	Estabelecimento de um *hub* remoto em São Paulo com estrutura de DIREx, bem como de ambientes para simulações virtual e construtiva
	Emprego da 2ª versão do Simulador de Planta Nuclear mediante cooperação com a Agência Internacional de Energia Atômica e com o CTMSP
Grupo de Estudo	Workshop sobre ações estratégicas no Setor Cibernético
	"Dia do Engajamento Ciber" com apresentações nas empresas sobre *Cyber Hygiene*
Cooperação Internacional	Parceria com o CCDCOE para emprego do Cenário 3 da ferramenta *Cyber Law Toolkit*, relacionado às implicações legais na proteção cibernética de infraestruturas críticas

Fonte: o autor (2019).

Figura 3 - Evolução do EGC



Fonte: o autor (2019).

3 CONCLUSÃO

O domínio cibernético perpassa a sociedade como um todo, provendo suporte para a economia global, infraestruturas críticas, segurança pública e defesa nacional, não respeitando fronteira física entre as nações.

Trata-se de um desafio que necessita de soluções estratégicas de longo prazo, requerendo ampla cooperação por meio do envolvimento de países, organismos internacionais, governo, Forças Armadas, comunidade acadêmica e setor privado.

O formato adotado no EGC contribui para incrementar a resiliência cibernética, por meio do estímulo à unidade de esforço entre os diversos atores civis e militares que constituem o ecossistema cibernético (EXÉRCITO BRASILEIRO, 2019b).

Como ensinamentos colhidos, destacam-se:

a)necessidade da rapidez e da oportunidade no compartilhamento de informação para fazer frente ao dinamismo e às incertezas das ameaças cibernéticas;

b) importância da troca permanente de experiências relacionadas às boas práticas*;*

c) conhecimento mútuo acerca das possibilidades e limitações dos diversos *stakeholders* que integram o espaço cibernético;

d) importância da Estratégia Nacional de Segurança Cibernética para a integração de iniciativas, alinhamento normativo e amadurecimento da sociedade quanto ao tema; e

e) identificação de subsídios para a melhoria do Plano Nacional de Tratamento de Incidentes de Redes.

Por fim, o EGC tem evoluído ao longo de suas edições, buscando agregar novos atores e reforçar a sinergia entre os envolvidos. O exercício representa a materialização da cooperação e integração entre o Sistema Militar de Defesa Cibernética e a proteção de infraestruturas críticas de interesse para a Defesa Nacional.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Livro Verde da Seguran**ça Cibernética. Brasília, DF: GSI, 2010.

_____. Gabinete de Segurança Institucional da Presidência da República. **Estratégia de Segurança da Informação e** Comunicações e de Segurança Cibernética da Administração Pública Federal. Brasília, DF: GSI, 2015.

_____. Gabinete de Segurança Institucional da Presidência da República. **Política Nacional de Segurança da Informação**. Brasília, DF: GSI, 2018.

_____. Gabinete de Segurança Institucional da Presidência da República. **Estratégia Nacional de Segurança Cibernética**. Disponível em: http://participa.br/seguranca-cibernetica/estrategia-nacional-de-seguranca-cibernetica-e-ciber. Acesso em 10 de outubro de 2019.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa**. Brasília, DF: Diário Oficial da União, 2008.

_____. Ministério da Defesa. **Diretriz do Ministério da Defesa Nr 14, Integração e Coordenação dos Setores Estratégicos de Defesa**. Brasília, DF: MD, 2009.

_____. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética (MD31-M-07)**. Brasília, DF: MD, 2014.

CCDCOE. **Cyberlaw Toolkit.** Disponível em: https://cyberlaw.ccdcoe.org/wiki/Scenario_03:_Cyber_operation_against_the_power_grid. Acesso em 10 de outubro de 2019.

E-ISAC. **Electricity Information Sharing and Analysis Center.** Analysis of the Cyber Attack on the Ukrainian Power Grid**.** Washington D.C., EUA: E-ISAC, 2016.

EXÉRCITO BRASILEIRO**. Noticiário do Exército sobre o Exercício Guardião Cibernético 2.0**. Disponível em: http://www.eb.mil.br/web/noticias/noticiario-do-exercito/-/asset_publisher/MjaG93KcunQI/content/id/9007697. Acesso em 10 de outubro de 2019a.

_____. Vídeo (4 min) do Exercício Guardião Cibernético 2.0. Disponível em: https://www.youtube.com/watch?v=a30GvHuYD64. Acesso em 10 de outubro de 2019b.

_____. **Guerra Cibernética (EB70-MC-10.232)**. Brasília, DF: EB, 2017.

NATO. Communications and Information Agency. **Malware Information Sharing Platform Leaflet**. Bruxelas, Bélgica, 2019.

*Tenente-Coronel **WALBERY** NOGUEIRA DE LIMA E SILVA é oficial de Estado-Maior do Comando de Defesa Cibernética e desempenhou a função de Coordenador Executivo do Exercício Guardião Cibernético (walbery.nogueira@eb.mil.br). Artigo realizado como trabalho de conclusão do Curso de Especialização em Planejamento de Guerra Eletrônica e Guerra Cibernética em Apoio às Operações, do Centro de Instrução de Guerra Eletrônica.