Segurança cibernética

Uma proposta de sistematização das Infraestruturas Críticas Nacionais

Brigadeiro da Reserva Pedro Arthur Linhares Lima, Professor Doutor,
Força Aérea Brasileira

Introdução

Com o advento da Era da Informação, também conhecida como Era Digital, e sua sucedânea, a Era do Conhecimento, a informação foi alçada à categoria de ativo estratégico para organizações e Estados-Nação, conferindo àqueles que a detém e dela se utilizam, efetiva e oportunamente, uma inquestionável vantagem no ambiente competitivo e nos contenciosos internacionais.

A Internet, proporcionando conectividade em tempo real e abrangência mundial, trouxe consigo crescimento sem precedentes no volume de informações disponíveis aos modernos decisores, mas, por outro lado, sua grande vulnerabilidade, aliada à existência de novos atores de funestas intenções no cenário internacional, fez crescer a preocupação com a proteção da informação que por ela trafega.

Segundo Mandarino[1], Infraestruturas Críticas (IC) são "as instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade".

A definição mais usual de IC é aquela que, uma vez prejudicada por fenômenos de causas naturais, como terremotos ou inundações ou por ações intencionais de sabotagem ou terrorismo, traz grandes reflexos negativos para toda uma nação e sua sociedade. São exemplos clássicos de IC: as redes telefônicas; os sistemas de captação e distribuição de água; e as fontes geradoras e as redes de distribuição de energia.[2]

Com um mundo hiperconectado, a vulnerabilidade das IC tornou-se um dos maiores desafios da atualidade, confirmado em análise apresentada pelo Boston Consulting Group.[3]

Desse modo, as evidências de riscos tecnológicos tratados no ambiente cibernético e direcionados às IC que se utilizam de Sistemas de Controle Industrial na monitorização de seus processos, ressaltam-se na medida em que tais sistemas vêm sofrendo significativa transformação, passando de sistemas de tecnologias proprietárias e isoladas para o emprego de arquiteturas abertas, estas interligadas, sobremaneira, com sistemas corporativos e com a rede mundial de computadores.[4]

Seguindo essa linha de raciocínio, qualquer impacto, seja ele positivo ou negativo, nas Infraestruturas Críticas Nacionais (ICN), irá afetar o Poder Nacional, que se traduz na capacidade que tem o conjunto de homens e dos meios que constituem a Nação, atuando em conformidade com a vontade nacional, para alcançar e manter os objetivos nacionais, manifestado nas cinco expressões: a política, a econômica, a psicossocial, a militar e a científico-tecnológica.

Dessa forma, é imperioso ao Estado se organizar para fazer frente a qualquer ação, seja ela natural ou intencional, que venha a colocar em risco uma IC. Por isso, este artigo propõe algumas alternativas estratégicas, visando contribuir para melhorar a estruturação, a sistematização e a integração das ICN com os órgãos estratégicos do governo e as Forças Armadas.

O ambiente cibernético e as ameaças às infraestruturas críticas

Com a evolução tecnológica, que acelerou, vertiginosamente, a capacidade de processamento automatizado de dados e o intercâmbio de informações entre pessoas e instituições, trazendo grandes benefícios à humanidade, por outro lado, possibilitou o aparecimento de ferramentas de intrusão nesses sistemas informatizados utilizados pelas pessoas no desenvolvimento de suas atividades particulares e profissionais.

Nos mais diversos níveis da gestão pública ou da gestão de negócios privados de interesse público, esses recursos informatizados são utilizados em atividades diversas, inclusive nos sistemas de controle de setores estratégicos de uma nação, como são as ICN de energia, telecomunicações, transportes, abastecimento de água, finanças e defesa, entre outras.

Analisando-se os ataques virtuais que tiveram como alvo as IC de alguns países, ocorridos na atualidade, verifica-se que a complexidade e o planejamento desses ataques tiveram como origem a vontade de fazer valer os interesses de alguns Estados sobre outros.

Nesse contexto, diversas ações de ataques cibernéticos contra redes de computadores e de comunicações utilizadas em sistemas estratégicos podem impactar até a segurança nacional, na medida em que podem interromper ou degenerar o funcionamento das estruturas essenciais à sociedade e ao estado brasileiro, como é o caso das ICN.

Ações relacionadas ao setor cibernético implementadas no Brasil

A Estratégia nacional de defesa e as ações de Segurança e Defesa Cibernética

A Estratégia Nacional de Defesa (END)[5] estabeleceu, em suas diretrizes, o fortalecimento de três setores de importância estratégica e essenciais para a defesa nacional: o espacial, o nuclear e o cibernético.

O mencionado Decreto também estabelece que as capacitações cibernéticas incluirão, como parte prioritária, as tecnologias de comunicações entre todos os contingentes das Forças Armadas, de modo a assegurar sua capacidade de atuar em rede.

A END enfatiza que os setores espacial e cibernético devem permitir que as forças Armadas, em conjunto, possam atuar em rede. Destaca também que todos os órgãos do Estado deverão contribuir para o incremento do nível de segurança nacional, com particular ênfase nos seguintes aspectos do Setor Cibernético: as medidas para a segurança das áreas de infraestruturas críticas; e o aperfeiçoamento dos dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos e, se for o caso, que permitam seu pronto estabelecimento.

Verifica-se, no contexto da END, que o Setor Cibernético não se restringe às atividades relacionadas à Segurança e Defesa Cibernética, mas abrange, também,

a Tecnologia da Informação e Comunicações (TIC), ferramenta básica para a implementação de redes de computadores.

Com base na END, pode-se listar os seguintes componentes básicos do Setor Cibernético para a sua atuação em rede: estrutura de comando, controle, comunicações, computação e inteligência (C4I) para a atuação operacional e o funcionamento administrativo das Forças Armadas; recursos de TIC; e arquitetura matricial que viabilize o transito de informações em apoio ao processo decisório em tempo quase real.

Segurança Cibernética

No nível político, as atividades relacionadas à Segurança da Informação e à Segurança Cibernética são tratadas pelos seguintes órgãos:

a. Conselho de Defesa Nacional (CDN)[6]: trata-se de um órgão de estado de consulta do Presidente da República nos assuntos relacionados à soberania nacional e à defesa do Estado democrático de direito. Tem sua secretaria executiva exercida pelo ministro-chefe do Gabinete de Segurança Institucional da Presidência da República (GSI-PR). As competências do CDN estão previstas no artigo 91 da Constituição Federal de 1988[7] e a regulamentação de sua organização e de seu funcionamento está contida na Lei nº 8.153, de 11 de abril de 1991[8];

b. Câmara de Relações Exteriores e Defesa Nacional (Creden): é um órgão de governo para o assessoramento do Presidente da República nos assuntos pertinentes às relações exteriores e à defesa nacional. Sua presidência cabe ao ministro-chefe do GSI-PR e, entre suas atribuições, encontra-se a segurança da informação, atividade essa que se insere no escopo do Setor Cibernético. Suas competências, organização e normas de funcionamento estão contidas no Decreto nº 4.801, de 6 de agosto de 2003[9];

c. Casa Civil da Presidência da República[10]: entre suas atribuições, merece destaque, por sua relação com o Setor Cibernético, aquela relacionada com a execução das políticas de certificados e normas técnicas e operacionais aprovadas pelo Comitê da Infraestrutura de Chaves Públicas Brasileiras (ICP-Brasil). Esta atribuição é da competência do Instituto Nacional de Tecnologia da Informação (ITI), uma autarquia federal vinculada à Casa Civil da Presidência da República, que tem o objetivo de manter a ICP-Brasil, que é a Autoridade Certificadora Raiz na cadeia de certificação;

d. Gabinete de Segurança Institucional da Presidência da República (GSI-PR)[11]: é o órgão da Presidência da República responsável pela coordenação, no âmbito da Administração Pública Federal (APF), de alguns assuntos es-

tratégicos que afetam a segurança da sociedade e do Estado, como: Segurança das ICN, SIC e Segurança Cibernética.

Para que possa cumprir a atribuição de coordenar as atividades de Segurança da Informação, o GSI-PR conta, em sua estrutura organizacional, com três órgãos subordinados, a saber:

a. Departamento de Segurança da Informação e Comunicações (DSIC): tem a atribuição de operacionalizar as atividades de Segurança da Informação e Comunicações (SIC) na APF, nos seguintes aspectos: regulamentar a SIC para toda a APF; capacitar os servidores federais, bem como os terceirizados, sobre SIC; realizar acordos internacionais de troca de informações sigilosas; representar o País junto à Organização dos Estados Americanos (OEA) para assuntos de terrorismo cibernético; e manter o Centro de Tratamento e Resposta a Incidentes de Redes da APF (CTIR-GOV).
b. Agência Brasileira de Inteligência (ABIN): é o órgão central do Sistema Brasileiro de Inteligência (SISBIN), que tem como objetivo estratégico desenvolver atividades de inteligência voltadas para a defesa do estado democrático de direito, da sociedade, da eficácia do poder público e da soberania nacional. Dentre as suas atribuições, a que envolve especificamente o Setor Cibernético, destaca-se a de avaliar as ameaças internas e externas à ordem constitucional, entre elas a cibernética.
c. Centro de Pesquisa e Desenvolvimento de Segurança das Comunicações (CEPESC): tem como atribuição buscar promover a pesquisa científica e tecnológica aplicada a projetos de segurança das comunicações.
d. Outro dispositivo importante que trata do assunto em pauta é o Decreto nº 3.505, de 13 de junho de 2000[12], que aprova a Política de Segurança da Informação para aplicação nos órgãos da Administração Pública Federal e confere à Secretaria-Executiva do CDN, assessorada pelo Comitê Gestor de Segurança da Informação, criado por esse mesmo Decreto, e apoiada pela ABIN, por intermédio de seu Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações, diversas atribuições para implementação de medidas relativas ao tema em lide.

Analisando esses dispositivos legais e o Decreto nº 9.031, de 12 de abril de 2017[13], que aprova a Estrutura Regimental do GSI-PR, verifica-se que o GSI-PR centraliza a coordenação da grande maioria das medidas relativas à Segurança Cibernética e suas áreas afins, de Segurança da Informação e das Comunicações e Segurança das Infraestruturas Críticas.

Além do já citado Comitê de Segurança da Informação, o GSI-PR coordena outros organismos importantes, como Grupos de Trabalho e Grupos Técnicos relacionados à Segurança das Infraestruturas Críticas, Segurança das Infraestruturas Críticas da Informação, Segurança Cibernética e Criptografia.

No tocante às ICN, a END seleciona seis áreas prioritárias, a saber: energia, telecomunicações, transportes, água, finanças e informação, sendo que, esta última, permeia todas ases anteriores, pois as IC dependem cada vez mais de redes de informação para a sua gerência e controle.

Defesa Cibernética

O Ministério da Defesa (MD) e as Forças Armadas, como membros da Administração Pública Federal, já participam ativamente do esforço nacional nas áreas de Segurança da Informação e Comunicações, Segurança Cibernética e Segurança das Infraestruturas Críticas.

Apesar da participação ativa nas áreas citadas, o MD vem capitaneando a ampliação dessas atividades e das estruturas e elas dedicadas, para atender ao amplo espectro das operações características de Defesa Cibernética, abrangendo:

a. no nível estratégico: as ações cibernéticas necessárias à atuação das Forças Armadas em situações de crise ou conflito armado e, até mesmo, em caráter episódico, em situação de paz ou normalidade institucional, ao receber mandato para isso, como aconteceu, por exemplo, na Copa do Mundo de 2014 e nos Jogos Olímpicos de 2016; e
b. no nível operacional: as ações cibernéticas, defensivas e ofensivas, relativas ao preparo (capacitação, adestramento ou treinamento) e ao emprego em operações militares, de qualquer natureza e intensidade, que caracterizam o ambiente de Guerra Cibernética.

A END formula diretrizes para o preparo e o emprego das Forças Armadas em atendimento às suas Hipóteses de Emprego (HE), definindo ações que devem ser observadas desde o tempo de paz, especialmente as relacionadas aos três setores estratégicos estabelecidos – o espacial, o cibernético e o nuclear.

Visando dar provimento ao estabelecido na END para esses setores estratégicos, o MD emitiu, em 9 de novembro de 2009, a Diretriz Ministerial nº 14[14], definindo responsabilidades sobre a coordenação e a liderança na condução das ações referentes aos setores nuclear, cibernético e espacial, respectivamente, à Marinha, ao Exército e à Aeronáutica.

Na referida Diretriz ficou estabelecido que os trabalhos fossem desenvolvidos em duas fases: na primeira, seriam definidos os objetivos de cada setor e a abrangência do

tema; e na segunda, seriam definidas as ações estratégicas e elaboradas as propostas de estruturas, com o máximo aproveitamento e adequação das já existentes.

No que se refere ao Setor Cibernético, o Exército concluiu a 1ª fase em dezembro de 2009, com base nos estudos e propostas de um Grupo de Trabalho (GT) interforças. Os trabalhos daquele grupo prosseguiram e o Exército concluiu a 2ª fase em março de 2010.

O MD aprovou as propostas do Exército, as quais estabeleceram os objetivos estratégicos a serem alcançados para o Setor Cibernético, juntamente com as ações estratégicas previstas para cada um deles[15].

Os objetivos estratégicos aprovados incluem ações voltadas, especialmente, para atividades de Segurança da Informação e Comunicações, Segurança Cibernética e Segurança das Infraestruturas Críticas, tanto no âmbito do MD quanto na participação colaborativa, no nível nacional, com as demais instituições envolvidas, em interação com estas, principalmente com o GSI-PR.

Essa participação colaborativa entre o MD e as instituições envolvidas, no nível nacional, pode ser colocada em prática nos dois últimos grandes eventos internacionais ocorridos no Brasil, que foram a Copa do Mundo de 2014 e os Jogos Olímpicos de 2016, conforme o modelo apresentado na Figura 1, onde, apesar da diversidade de organizações envolvidas, os trabalhos ocorreram com fluidez, colaborando para o sucesso desses eventos.

Figura 1 – Modelo de participação colaborativa empregado nos dois últimos grandes eventos ocorridos no Brasil (Fonte: disponibilizado pelo ComDCiber, em 18 ago. 2018)

Na área de Defesa Cibernética, cumpre destacar duas ações estratégicas, já consolidadas, referentes ao Objetivo Estratégico nº 1, que estabelece a criação de uma estrutura de Defesa Cibernética subordinada ao Estado-Maior Conjunto das Forças Armadas para inserir o tema nos planejamentos militares conjuntos e a criação do Comando de Defesa Cibernética das Forças Armadas (ComDCiber) para dar execução aos objetivos estratégicos estabelecidos para o setor e suas ações estratégicas correspondentes.

Sob a coordenação do Núcleo do ComDCiber, a partir de 2015, e após a sua efetivação, em 2016, várias Ações Setoriais de Defesa já foram consolidadas, como a implantação do Sistema Militar de Defesa Cibernética, e várias outras foram iniciadas, como a promoção da interoperabilidade do Setor Cibernético na Defesa Nacional, a criação e implantação da Escola Nacional de Defesa Cibernética, a criação e implantação do Sistema de Homologação e Certificação de Produtos de Defesa Cibernética, a capacitação e geração de recursos humanos necessários à condução das atividades do Setor Cibernético no âmbito da Defesa Nacional, a implantação do Sistema de Informações Seguras, com enfoque na área de SIC, a contribuição para o fomento da pesquisa e do desenvolvimento de produtos de defesa e a contribuição para a produção do conhecimento de inteligência oriundo da fonte cibernética.

Como podemos perceber, na área de Defesa Cibernética, já estão estabelecidos os parâmetros básicos para a expansão, o aprimoramento e a consolidação do setor, em atendimento ao estabelecido na END e às demandas para alcançar uma estrutura sistêmica eficaz, no âmbito nacional.

Ações propostas

Analisando a situação atual da Segurança e Defesa Cibernética no Brasil, constatamos que existem várias normas que estruturam e orientam o setor e, ainda assim, não temos os órgãos que compõem as ICN, os órgãos estratégicos do Governo e o Ministério da Defesa integrados e interagindo de forma sistêmica. Perguntamos: por que ainda não foi possível essa integração mais estreita de todos os entes envolvidos nesse processo? O que será que está faltando? Para tentar responder a esses questionamentos, serão propostas, a seguir, algumas sugestões de ações.

Com relação à Segurança Cibernética, como foi mostrado, várias ações já foram tomadas visando proteger e garantir a utilização de ativos de informação estratégicos, principalmente os ligados às infraestruturas críticas da informação que controlam as ICN. Entretanto, não se conseguiu, ainda, uma interação efetiva que proporcione a tão almejada integração de todos os ór-

gãos públicos e privados envolvidos no funcionamento das ICN, especialmente os órgãos da APF.

Nesse sentido, é imperioso que todos os entes envolvidos com a Segurança Cibernética das ICN implementem também ações que garantam, primeiramente, que seus ativos críticos de informação estejam minimamente protegidos contra as ameaças internas e externas. Para isso, devem promover ações internas, ou seja, dentro de seus próprios órgãos, de modo a diminuir as fragilidades de seus ativos de informação contra ataques mal intencionados e aumentar a sua resiliência.

Sistemática para Avaliação e Gerenciamento de Riscos e Continuidade de Negócios

Como primeiro passo para diminuir as fragilidades de seus ativos informacionais, é necessário realizar uma avaliação de riscos. Somente após essa avaliação, ter-se-á uma noção das ações que devam ser tomadas para que se possa minimizar os riscos encontrados.

Indo ao encontro desse objetivo, e visando orientar todos os órgãos da APF, o GSI-PR publicou, em 2010, o "Guia de Referência para a Segurança das Infraestruturas Críticas da Informação - Versão 01"[16]. Esse Guia, além da caracterização e contextualização do tema segurança das infraestruturas críticas da informação, apresenta uma sistemática para avaliação de riscos com proposta mais detalhada de gerenciamento de riscos e continuidade de negócios.

As ações propostas nesse Guia devem ser executadas por todos os órgãos envolvidos no processo de proteção das ICN, pois são fundamentais para a realização do próximo passo, que abrange a implantação de centros e equipes de monitoramento de ameaças, que permitirá a interação e a troca de informações com os órgãos de acompanhamento e controle.

Criação de Centros e Equipes de Tratamento de Incidentes de Redes (CTIR e ETIR)

Com a finalidade precípua de atender aos incidentes em redes de computadores pertencentes à APF, o Departamento de Segurança da Informação e Comunicações (DSIC) do GSI-PR instituiu o CTIR Gov, que é o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal.

Compete ao CTIR Gov, por intermédio da Coordenação-Geral de Tratamento de Incidentes de Redes (CGTIC)[17]: operar e manter o Centro de

Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal-CTIR Gov; promover o intercâmbio científico-tecnológico relacionado a incidentes de segurança de redes de computadores junto a outros centros; apoiar órgãos e entidades da administração pública federal nas atividades de tratamento de incidentes de segurança de redes de computadores; monitorar e analisar tecnicamente os incidentes de segurança nas redes de computadores da administração pública federal; implementar mecanismos que permitam a avaliação dos danos ocasionados por incidentes de segurança nas redes de computadores da administração pública federal; e apoiar, incentivar e contribuir no âmbito da administração pública federal para a capacitação no tratamento de incidentes de segurança em redes de computadores.

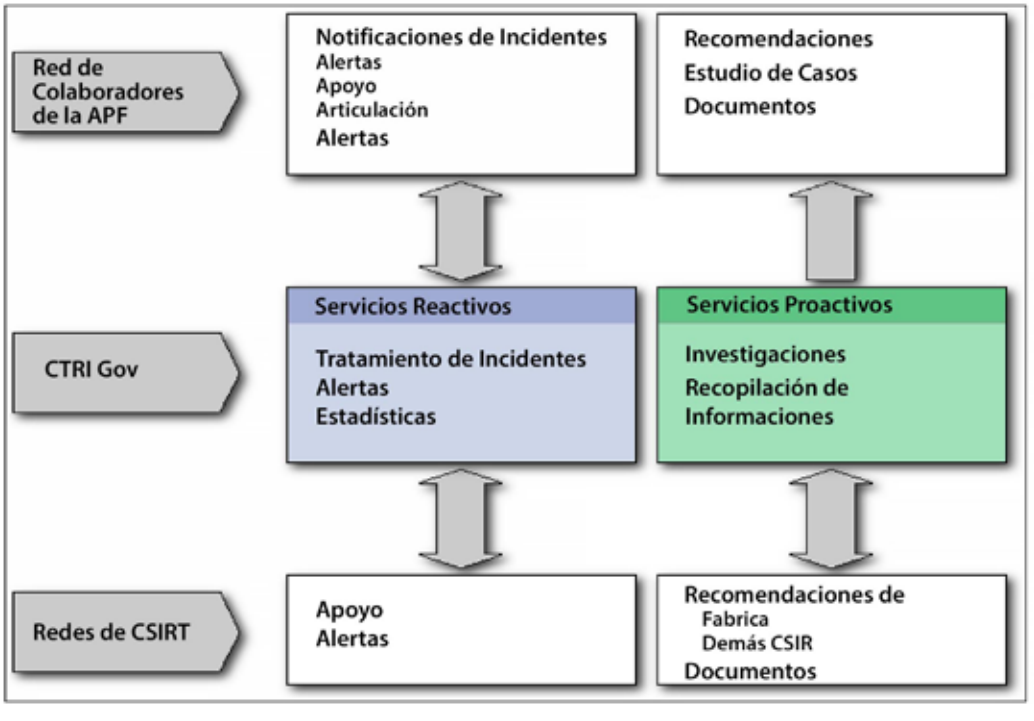

Figura 2 - Interações do CTIR Gov

Um incidente de segurança é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores. O processo de tratamento de incidentes, conforme apresentado na Figura 2, é, basicamente, desdobrado em:

a. Notificação do Incidente: o recebimento de notificações de incidentes permite ao CTIR Gov atuar como ponto central para coordenação de soluções dos problemas decorrentes, por meio da coleta de atividades e incidentes reportados, análise das informações e correlação destas no âmbito da organização informante ou da comunidade da APF. As informações podem ser utilizadas também para determinar tendências e padrões de atividades de ataques e para recomendar estratégias de prevenção adequadas para toda a APF;

b. Análise de Incidentes: esta atividade consiste em examinar todas as informações disponíveis sobre o incidente, incluindo artefatos e outras evidências relacionadas ao evento. O propósito da análise é identificar o escopo do incidente, sua extensão, sua natureza e quais os prejuízos causados. Também faz parte da análise do incidente propor estratégias de contenção e recuperação;

c. Suporte à Resposta a Incidentes: neste caso, o CTIR Gov auxilia no processo de recuperação. Esse auxílio é prestado por e-mail ou pela indicação de documentos que possam auxiliar no processo de recuperação. Essa atividade pode envolver o auxílio na interpretação dos dados coletados e na recomendação de estratégias de contenção e recuperação;

d. Coordenação na Resposta a Incidentes: nesta atividade, o CTIR Gov coordena as ações entre os envolvidos em um incidente, o que pode incluir redes e outros centros de tratamento (CSIRTs) externos ao seu âmbito de atuação. O processo de coordenação envolve a coleta de informações de contato, a notificação dos responsáveis pelas redes, computadores ou sistemas que possam estar envolvidos ou comprometidos e a geração de indicadores e estatísticas relativas aos incidentes. O CTIR Gov age como um facilitador no processo de recuperação dos incidentes e na troca de informações entre as partes envolvidas;

e. Distribuição de Alertas, Recomendações e Estatísticas: esta atividade consiste em disseminar informações relativas a novos ataques ou tendências de ataques observadas pelo CTIR Gov, por outros centros de tratamento ou por empresas especializadas. Esses alertas, em geral, são produzidos pelo próprio CTIR Gov, baseados nas notificações recebidas ou em incidentes tratados, ou são redistribuições de alertas emitidos por outros Centros com responsabilidade nacional. O CTIR Gov, ao redistribuir alertas, pode acrescentar recomendações específicas para seu público e atribuir diferentes graus de severidade; e

f. Cooperação com outras Equipes: o CTIR Gov, por meio da Coordenação-Geral, atua na implementação de acordos de cooperação com outras Equipes de Tratamento de Incidente da APF, bem como com outros CSIRTs, públicos e privados, nacionais e internacionais, visando à cooperação técnica e à ajuda mútua no tratamento de incidentes de segurança.

Por intermédio da Instrução Normativa nº 1[18], o GSI-PR orienta os órgãos e entidades da Administração Pública Federal, direta e indireta, descriminando todas as ações necessárias para se implementar a Gestão de Segurança da Informação e Comunicações. Dentre essas orientações, pode-se destacar: nomear Gestor de SIC; instituir e implementar Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR); e aprovar Política de SIC e demais normas de segurança da informação e comunicações.

Com relação à criação das ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta, o GSI-PR editou a Norma Complementar Nº 5[19] disciplinando a criação dessas Equipes.

Nessa Norma Complementar, além de oferecer vários modelos de implementação das ETIR, apresenta muitas maneiras diferentes dessas Equipes serem estruturadas, dependendo do modelo de implementação a ser adotado, do tamanho da organização, do número de localizações geográficas distribuídas e onde as funções estão localizadas, do número de sistemas e plataformas suportados, do número de serviços a serem oferecidos e do conhecimento técnico do pessoal existente.

Assim como as Normas citadas acima, o GSI-PR editou várias outras Normas Complementares que vêm auxiliando todos os órgãos da APF a se estruturarem e operacionalizarem a proteção de suas redes computacionais.

Aproveitando toda essa experiência exitosa da APF, propõe-se que todos os entes que compõem as ICN adotem essa mesma estrutura para o tratamento dos incidentes de rede computacionais, ou seja: implementação de CTIR e ETIR em todos os atores que lidam com a segurança das infraestruturas críticas do País.

Uma forma de se implementar essa estrutura seria:

a. Criação de um CTIR em cada Agência Reguladora das áreas prioritárias, como por exemplo: Comunicações (ANATEL), Energia (ANEEL), Água (ANA), Transportes (ANTT).

b. Criação das ETIR nos diversos órgãos que compõem as ICN, por exemplo, energia elétrica: uma ETIR em cada uma das Operadoras, Distribuidoras, Transmissoras e Geradoras de energia elétrica, ligadas ao CTIR da ANEEL.

c. Ligação de todos os CTIR, incluindo aqui o Comando de Defesa Cibernética (ComDCiber), que atuaria como um CTIR do Ministério da Defesa, ao CTIR Gov ou outro órgão que possa vir a ser criado para esse fim. Nesse caso, o CTIR Gov também estaria ligado a esse órgão.

Com a criação desses CTIR e ETIR, estariam abertas as portas para uma maior interação entre todos os entes ligados à Segurança e Defesa Cibernética das ICN e estaria, também, lançada a base para a criação e efetivação de um Sistema de Segurança e Defesa Cibernética Brasileiro.

Criação do Sistema de Segurança e Defesa Cibernética Brasileiro

Como se pode observar do que foi até aqui apresentado, o Brasil já possui uma estrutura básica significativa nas áreas de Segurança Cibernética (aqui incluída a Segurança da Informação e das Comunicações e Segurança das Infraestruturas Críticas) e Defesa Cibernética.

Na área de Segurança Cibernética, a estrutura atual confere vantagem fundamental ao concentrar a coordenação das ações principais num órgão da estrutura da Presidência da República, no caso o GSI-PR.

O trabalho do GSI-PR nesse setor é facilitado pela sua estrutura organizacional que permite congregar esforços das principais áreas de interesse, reunindo os campos técnicos da atividade à inteligência, à prevenção e gerenciamento de crises e ao campo militar.

Outro fator relevante é a responsabilidade atribuída ao GSI-PR de executar as atividades necessárias ao exercício das competências do CDN e da Creden, organismos que detêm prerrogativas essenciais voltadas ao Setor Cibernético nos campos das decisões estratégicas, no caso a CDN, e da formulação das políticas públicas e diretrizes, bem como da articulação de ações que envolvam mais de um ministério, nesse caso o Creden.

Portanto, é desejável que se mantenham todas essas atribuições vinculadas a um órgão da estrutura da Presidência da República, no caso atual o GSI-PR, que atuaria como Órgão Central desse Sistema.

Isso se aplica, também, às atividades de Defesa Cibernética, que embora sejam mais diretamente ligadas ao Ministério da Defesa e às Forças Armadas, necessitam da vinculação ao CDN, para as decisões estratégicas, e à Creden, principalmente para a articulação de ações com outros órgãos públicos e privados de interesse.

Tomando-se como ponto de partida as propostas apresentadas por OLIVEIRA[20], propõe-se o fortalecimento das estruturas já existentes e a adoção de mecanismos que proporcionem a sua atuação sistêmica, como a formulação das

políticas e diretrizes públicas correspondentes e da emissão de dispositivos legais que amparem e regulamentem a atuação articulada dos órgãos participantes do sistema.

Figura 3 – Modelo Institucional do Sistema de Segurança e Defesa Cibernética Brasileiro (adaptado BARROS)

De uma forma simplificada, a Figura 3 apresenta uma visão geral do Modelo Institucional do Sistema de Segurança e Defesa Cibernética Brasileiro, adaptado BARROS.

Quanto à Defesa Cibernética, os objetivos estratégicos e ações estratégicas correspondentes já estão estabelecidos, conforme explanado anteriormente, trata-se agora de buscar implementá-los.

Para viabilizar a criação desse Sistema e facilitar os entendimentos para a sua implementação, torna-se necessário o estabelecimento de um Grupo de Trabalho interministerial de alto nível, no âmbito da Creden, a fim de estudar e propor a organização desse novo Sistema, com base na expansão, adequação e aprimoramento das estruturas existentes.

Outro ponto importante a destacar é a imperiosa necessidade do Sistema contemplar a participação e a interação permanentes com a atividade de inteligência.

Integração das atividades de Inteligência à Segurança e DefesaCibernética

A atividade de inteligência exerce papel fundamental nos ambientes de Segurança e Defesa Cibernética. Ela é essencial na busca de informações, empregando todas as fontes disponíveis, para identificar e prevenir ameaças cibernéticas e proporcionar respostas adequadas, com oportunidade. Além disso, os profissionais que atuam no Setor Cibernético devem desenvolver atitude intrínseca de contrainteligência, a fim de proteger o conhecimento e as informações inerentes às suas atividades.

Nesse particular, é importante a expansão das atividades de Inteligência do Sinal para abranger, também, as necessidades cibernéticas, como está ocorrendo em outros países. Poder-se-ia aproveitar a experiência de atuação nesse ambiente das Forças Armadas e do SISBIN.

Portanto, os órgãos de inteligência do SISBIN devem cumprir atividades importantes, dentro do pretendido Sistema de Segurança e Defesa Cibernética Brasileiro.

Considerações Finais

Se, por um lado, os avanços obtidos na área de Tecnologia da Informação e das Comunicações facilitam nossas vidas e trazem benefícios importantes para a humanidade como um todo, por outro lado, trazem, também, efeitos colaterais nocivos com os quais temos que aprender a lidar.

Assim como o espaço cibernético evolui, é de se esperar que as ameaças e os desafios que emanam dele também evoluam.

A ameaça cibernética é patente e real. Ela se revela na rotina das pessoas e instituições, quer nos ambientes individual, coletivo ou profissional, e se estampa no noticiário da mídia praticamente todos os dias.

No ambiente estratégico do Estado, o combate a essa ameaça deve fazer parte de suas prioridades, a fim de prevenir danos à sociedade e ao próprio Estado, os quais podem assumir proporções consideráveis.

No Brasil, apesar de ser relativamente recente a preocupação com o tema, as ações têm-se intensificado nos últimos anos.

No campo da Segurança Cibernética, as ações ganharam maior impulso a partir da criação do DSIC no GSI-PR, em 2006, e no campo da Defesa Cibernética, ênfase maior passou a ser observada a partir da edição da END, em 2008.

De qualquer modo, o momento atual é propício para acelerar medidas, a fim de se melhorar a interação e integração de todos os atores que lidam com a segurança das infraestruturas críticas nacional e que comporiam o Sistema de

Segurança e Defesa Cibernética Brasileiro. Nesse sentido, foram propostas algumas ações para contribuir com o alcance desses objetivos:

a. Sistemática para Avaliação e Gerenciamento de Riscos e Continuidade de Negócios, como sendo o primeiro passo para a proteção dos ativos críticos da informação;
b. Criação de Centros e Equipes de Tratamento de Incidentes de Redes (CTIR e ETIR), como uma forma de se facilitar a interação e a troca de informações entre todos os entes envolvidos na proteção das ICN;
c. Criação do Sistema de Segurança e Defesa Cibernética Brasileiro, para sistematizar, integrar e permitir que as informações fluam com rapidez, para que os atores responsáveis possam tomar as decisões acertadas tempestivamente, e estabelecer um ambiente colaborativo permanente; e
d. Integração das atividades de Inteligência à Segurança e Defesa Cibernética, como uma forma de se prever, antever e até impedir que as tentativas de ataques aconteçam. De uma forma geral, este trabalho procurou focar na melhoria das interações e integração dos órgãos que compõem a ICN, com relação à Segurança e Defesa Cibernética. Assim, para a estruturação e fortalecimento da proteção cibernética das ICN, vários outros fatores, além das propostas aqui apresentadas, devem ser considerados e analisados pelo Grupo de Trabalho Interministerial, proposto acima, uma vez que fugiriam ao escopo deste trabalho.

De uma forma geral, este trabalho procurou focar na melhoria das interações e integração dos órgãos que compõem a ICN, com relação à Segurança e Defesa Cibernética. Assim, para a estruturação e fortalecimento da proteção cibernética das ICN, vários outros fatores, além das propostas aqui apresentadas, devem ser considerados e analisados pelo Grupo de Trabalho Interministerial, proposto acima, uma vez que fugiriam ao escopo deste trabalho. ❑

Notas

1. MANDARINO JR., Raphael. Segurança e Defesa do Espaço Cibernético Brasileiro. Brasília. 2010. p. 38.

2. International Critical Information Infrastructures Protection Handbook 2008/2009. Center for Security Studies, ETH Zurich, p. 36-37. Apud CANONGIA, Claudia, março 2009.

3. Boston Consulting Group, World Economic Forum in "Our Critical Infraestructure is More Vulnerable than Ever". Disponível em: <https://www.weforum.org/agenda/2017/02/our-critical-infrastructure-is-more-vulnerable-than-ever-it-doesn-t-have-to-be-that-way/>, Acesso em: 12 ago. 2018.

4. ENISA, Protecting Industrial Control Systems. Recommendations for Europe and Member States. 2011. Disponível em: < https://www.enisa.europa.eu/publications/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states>. Acesso em: 12 ago. 2018.

5. BRASIL. Presidência da República. Decreto nº 6.703. Aprova a Estratégia Nacional de Defesa, e dá outras providências. Brasília. Diário Oficial da União, Poder Executivo. Brasília. 19 dez. 2008. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Decreto/D6703.htm>. Acesso em: 12 ago. 2018.

6. BRASIL. Presidência da República. Lei nº 8.153. Dispõe sobre a organização e o funcionamento do Conselho de Defesa Nacional e dá outras providências. Brasília. 11 abr. 1991. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L8183.htm>. Acesso em: 12 ago. 2018.

7. BRASIL. Constituição da República Federativa do Brasil. Brasília. 1988. Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 12 ago. 2018.

8. BRASIL. Presidência da República. Lei nº 8.183. Organização e funcionamento do Conselho de Defesa Nacional - CDN. Brasília. 11 abr. 1991. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L8183.htm>. Acesso em: 12 ago. 2018.

9. BRASIL. Presidência da República. Decreto nº 4.801. Cria a Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo. Brasília. 6 ago. 2003. Disponível em: <http://www.planalto.gov.br/ccivil_03/Decreto/2003/D4801.htm>. Acesso em: 12 ago. 2018.

10. BRASIL. Lei nº 13.502, de 1º de novembro de 2017. Estabelece a organização básica dos órgãos da Presidência da República e dos Ministérios. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/Lei/L13502.htm>. Acesso em: 12 ago. 2018.

11. BRASIL. Decreto nº 9.031, de 12 de abril de 2017. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Gabinete de Segurança Institucional da Presidência da República. Disponível em: <http://planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Decreto/D9031.htm>. Acesso em: 12 ago. 2018.

12. BRASIL. Presidência da República. Decreto nº 3.505. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Brasília. 13 jun. 2000. Disponível em: <http://www2.camara.leg.br/legin/fed/decret/2000/decreto-3505-13-junho-2000-368759-publicacaooriginal-1-pe.html>. Acesso em: 12 ago. 2018.

13. BRASIL. Presidência da República. Decreto nº 9.031. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Gabinete de Segurança Institucional da Presidência da República. Brasília. 12 abr. 2017. Disponível em: <http://planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Decreto/D9031.htm>. Acesso em: 12 ago. 2018.

14. BRASIL. Ministério da Defesa. Diretriz Ministerial nº 14. Integração e Coordenação dos Setores Estratégicos de Defesa. Brasília. 9 nov. 2009. Disponível em: <https://www.defesa.gov.br/arquivos/File/legislacao/emcfa/portarias/0014_2009.pdf>. Acesso em: 18 ago. 2018.

15. BRASIL. Ministério da Defesa. Portaria Normativa nº 2.621. Aprova a Estratégia Setorial de Defesa. Brasília. 7 dez. 2015. Disponível em: <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=09/12/2015&jornal=1&pagina=32&totalArquivos=136>. Acesso em: 18 ago. 2018.

16. BRASIL. Presidência da República. Gabinete de Segurança Institucional da Presidência da República. Guia de Referência para a Segurança das Infraestruturas Críticas da Informação.

Versão 1. Brasília. nov. 2010. Disponível em: <http://dsic.planalto.gov.br/legislacao/2_Guia_SICI.pdf>. Acesso em: 12 ago. 2018.

17. BRASIL. Presidência da República. Gabinete de Segurança Institucional da Presidência da República. Portaria nº 13. Brasília. 4 ago. 2006.

18. BRASIL. Presidência da República. Gabinete de Segurança Institucional da Presidência da República. Instrução Normativa nº 1. Brasília. 13 jun. 2008. Disponível em: <https://www.governodigital.gov.br/documentos-e-arquivos/legislacao/14_IN_01_gsidsic.pdf>. Acesso em: 19 ago. 2018.

19. BRASIL. Presidência da República. Gabinete de Segurança Institucional da Presidência da República. Norma Complementar nº 5. Brasília. 14 ago. 2009. Disponível em: <http://dsic.planalto.gov.br/legislacao/nc_05_etir.pdf>. Acesso em: 19 ago. 2018

20. OLIVEIRA, J.R. Sistema de Segurança e Defesa Cibernética Nacional: Abordagem Com Foco nas Atividades Relacionadas à Defesa Nacional. In: Desafios Estratégicos Para a Segurança e Defesa Cibernética. 1ª Edição. 2011. Brasília. Anais Brasília: Imprensa Nacional, 2011.

Brigadeiro Intendente da Reserva Pedro Arthur Linhares Lima, Professor Doutor, Força Aérea Brasileira

Graduado pela Academia da Força Aérea. Extensão em Análise de Sistemas na PUC-RJ. Mestre em Ciências da Computação no Air Force Institute of Technology – USA. Doutor em Ciências em Engenharia de Produção pela COPPE/UFRJ. MBA em Política e estratégia pela COPPEAD-UFRJ. Foi Chefe do Centro de Computação da Aeronáutica de São José dos Campos; Subdiretor de Sistemas e Infraestrutura de TI, Subdiretor de Projetos de TI, Assessor-Chefe de Governança de TI e Diretor de Tecnologia da Informação da Aeronáutica. Atualmente é Pesquisador e Professor do Programa de Pós-graduação em Ciências Aeroespaciais da Universidade da Força Aérea – UNIFA.