Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Estudo sobre Hardware Trojans e suas ameaças à Administração Pública Federal

Gustavo A. Bruzzeguez

Dissertação apresentada como requisito parcial para conclusão do
Mestrado Profissional em Computação Aplicada

Orientador
Prof. Dr. João Carlos Félix Souza

Coorientador
Prof. Dr. Clóvis Neumann

Brasília
2017

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

AG982e

Andrade Bruzzeguez, Gustavo
Estudo sobre Hardware Trojans e suas ameaças à Administração Pública Federal / Gustavo Andrade Bruzzeguez; orientador João Carlos Félix Souza; co-orientador Clóvis Neumann. -- Brasília, 2017.
120 p.

Dissertação (Mestrado - Mestrado Profissional em Computação Aplicada) -- Universidade de Brasília, 2017.

1. Segurança da Informação e Comunicação. 2. Segurança Cibernética. 3. Hardware Trojan. I. Félix Souza, João Carlos, orient. II. Neumann, Clóvis , co-orient. III. Título.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Estudo sobre Hardware Trojans e suas ameaças à Administração Pública Federal

Gustavo A. Bruzzeguez

Dissertação apresentada como requisito parcial para conclusão do
Mestrado Profissional em Computação Aplicada

Prof. Dr. João Carlos Félix Souza (Orientador)
CIC/UnB

Dr.a Elaine C. Marcial
Instituto de Pesquisa Econômica Aplicada

Prof.a Dr.a Simone B. S. Monteiro
Universidade de Brasília

Prof. Dr. Marcelo Ladeira
Coordenador do Programa de Pós-graduação em Computação Aplicada

Brasília, 15 de dezembro de 2017

Dedicatória

Dedico esse trabalho e essa conquista às minhas filhas: Ana Clara e Helena. Que o respeito a Deus, o trabalho honesto, a dedicação aos estudos e o cultivo de valores do bem possam ser sempre o norte em suas vidas.

Agradecimentos

Deus nos dá o dom da vida, autorizando nossa permanência nesse mundo. A Ele, que nos permite sonhar, lutar e conquistar, meu primeiro agradecimento!

Mas um mestrado, embora seja por vezes um exercício solitário de incontáveis madrugadas, não se constrói sozinho. Várias atores influenciaram essa jornada.

Então prossigo e agradeço, acima de tudo, à minha família: ao meu pai, que nos deu o exemplo de honestidade, humildade e competência; à minha mãe, que com tanto carinho cuidou de nós e sempre procurou nos alertar e ensinar sobre a vida; ao meu irmão, Éverton, que sempre foi um grande exemplo pra mim (o "irmão mais velho") e influenciou, deveras, meu caminho; e à minha irmãzinha Évila, companheira de tantos e tantos momentos, que sempre admirou o meu esforço e sempre me motivou a estudar e a ir além.

À minha esposa Angélica, minha companheira de tantos anos, cujo suporte foi fundamental para que eu conseguisse edificar esse trabalho, apesar dos incontáveis momentos extraídos de seu convívio.

Às minhas filhas Ana Clara e Helena, meu obrigado por me lembrarem, sempre, que a felicidade é algo muito simples!

Aos meus orientadores, Dr. João Carlos Félix (Joca) e Dr. Clóvis Neumann, por terem acreditado na minha ideia e no meu trabalho, e por terem ajudado muito, com paciência e dedicação.

Ao Prof. Dr. Marcelo Ladeira, pelo apoio, e por acreditar que é possível transformar a Administração Pública no Brasil.

Às professoras Dra. Simone Borges, Dra. Ana Carla e Dra. Elaine Coutinho, pelas observações pertinentes que permitiram o aprimoramento desse trabalho.

Ao General Marconi, do DSIC/GSI/PR, ao Antonio Futuro, da SOF/MP, e à Dra. Maria Aparecida Siqueira, da AGU/PR, por terem me apoiado, institucionalmente, a seguir em frente com esse trabalho.

Agradeço ao amigo Carlos Maurício, Major do Exército Brasileiro, que tanto me incentivou a seguir com esse projeto.

Ao amigo Tenente-Coronel Fraide, pelos *insights* e reflexões sobre inteligência e segurança cibernética.

Ao amigo Degnaldo, que também me inspirou por ter vivido semelhante desafio com seu mestrado.

Agradeço à amiga Leila Frossard, pelas valiosas observações sobre meu tema em artigos.

Aos colegas de trabalho Augusto Cantanhede, Antonio Netto, Bruno Fassheber e Michele Costa L., pelo incentivo ao meu trabalho, pelo compartilhamento de experiências ou por apenas terem me ouvido.

Aos colegas de UnB e de luta: Clayton, Carol, Cristina, Tassio e tantos outros, pelos momentos de parceria e descontração em meio aos desafios do mestrado.

Resumo

Nos últimos anos, pesquisadores vêm demonstrando a possibilidade de implementação de códigos maliciosos em circuitos integrados durante a fabricação destes dispositivos. A ameaça, que ficou conhecida como hardware trojan, vem atraindo a atenção dos governos e da indústria, dado que potencialmente envolve questões de espionagem e guerra cibernética. Diversos estudos vem sendo desenvolvidos na comunidade acadêmica mundial, em particular nos últimos 5 anos, conforme se constatou no levantamento bibliográfico com uso do enfoque meta-analítico. Não obstante, no Brasil, pouco se tem falado sobre o tema. Recentemente, o Gabinete de Segurança Institucional da Presidência da República publicou a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018, o que demonstra a vontade do Estado brasileiro em equacionar os problemas afetos à área cibernética, por meio do planejamento e da coordenação de esforços dos órgãos públicos, em parceria com a sociedade. Trabalhando a partir dos Objetivos Estratégicos declarados nessa Estratégia, e utilizando-se de conceitos do Balanced Scorecard e da metodologia 5W2H, o trabalho propôs desdobramentos, no nível tático, de tais Objetivos, de forma que a Estratégia possa também abordar as questões associadas à ameaça do hardware Trojan. Não obstante os avanços notados na área cibernética, observa-se que o país encontra-se vulnerável à ameaça do hardware Trojan, seja pela incapacidade de detecção da ameaça, seja pela ausência de ações governamentais focando especificamente o problema.

Palavras-chave: segurança da informação, segurança cibernética, hardware Trojan

Abstract

In recent years, researchers have been demonstrating the possibility of malicious code being introduced into integrated circuits during the fabrication of these devices. The threat, which has become known as hardware Trojan, has attracted the attention of governments and industry as it potentially involves espionage and cyber warfare issues. Several studies have been developed in the world academic community, in particular in the last 5 years, as was verified in the bibliographical survey using the meta-analytic approach. Nevertheless, in Brazil, little has been said about the subject. Recently, the Office of Institutional Security of the brazilian Presidency of the Republic has published the Strategy for Information Security and Cybersecurity of the Federal Public Administration 2015-2018, which demonstrates the Brazilian State's willingness to address the problems to the cybernetic area, through the planning and coordination of efforts of public agencies, in partnership with society. Working from the Strategic Objectives stated in this Strategy, and using concepts from the Balanced Scorecard and the 5W2H methodology, the work proposed a tactical level development of these Objectives, so that the Strategy could also address issues associated with the hardware Trojan threat. Despite the notable advances in the area of cybernetics, it's noted that the country is vulnerable to the threat of hardware Trojan, either by the inability to detect the threat or by the absence of government actions specifically focusing on the problem.

Keywords: information security, cyber security, hardware Trojan

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

ABIN Agência Brasileira de Inteligência

APF Administração Pública Federal

CAPES Coordenação de Aperfeiçoamento de Pessoal de Nível Superior

CDCiber Comando de Defesa Cibernética

CDN Conselho de Defesa Nacional

Cepesc Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações

CGSI Comitê Gestor de Segurança da Informação

CI Circuito Integrado

CIA Central Intelligence Agency

CIC Departamento de Ciência da Computação

CPI Comissão Parlamentar de Inquérito

CREDEN Câmara de Relações Exteriores e Defesa Nacional

DoS Denial of Service

EDA Electronic Design Automation

ENaDCiber Escola Nacional de Defesa Cibernética

ENAP Escola Nacional de Administração Pública

GSI Gabinete de Segurança Institucional

HT Hardware Trojan

IP Intellectual Property

MCTIC Ministério da Ciência, Tecnologia, Inovações e Comunicações

MD Ministério da Defesa

MDIC Ministério da Indústria, Comércio Exterior e Serviços

MP Ministério do Planejamento, Desenvolvimento e Gestão

MRE Ministério das Relações Exteriores

NSA National Security Agency

PADIS Programa de Apoio ao Desenvolvimento Tecnológico da Indústria de Semicondutores

PPA Plano Plurianual

PR Presidência da República

SegCiber Segurança Cibernética

SEM Scanning Electron Microscope

SIC Segurança da Informação e Comunicação

SISBIN Sistema Brasileiro de Inteligência

SoC System on a Chip

TAPO Trusted Access Program Office

UnB Universidade de Brasília

Capítulo 1

Introdução

1.1 Contextualização

A segurança cibernética, desafio do século XXI, vem se destacando como função estratégica de Estado, sendo essencial à manutenção das infraestruturas críticas de um país, tais como energia, defesa, transportes, telecomunicações, finanças, da própria informação, dentre outras [1].

As questões ligadas à segurança cibernética são complexas e sofisticadas porque estão em constante transformação, ou seja, quando se imagina ter equacionado determinado problema, o problema ou o ambiente costumam se alterar [2].

As falhas de segurança e privacidade que vieram à tona nos últimos anos vem enfraquecendo a confiança do público na tecnologia de forma geral, e a rápida implementação de novas tecnologias apenas agrava essa condição [3].

Casos mais recentes e de grande impacto, tais como o *worm*[1] Stuxnet (2010), ataque que atingiu o sistema de controle industrial das instalações nucleares iranianas [5]; a invasão da multinacional Sony (2011), que expôs dados de 77 milhões de contas de usuários mantidas pela empresa [6]; o ataque cibernético à rede de TV francesa TV5Monde (2015), que corrompeu diversos sistemas da emissora, tirando-a do ar [7]; e os recentes *ransomwares*[2] Wannacry, Petya e Bad Rabbit (2017), ameaças que se espalharam nas redes de computadores no mundo todo, "sequestrando"arquivos de computador em troca

[1]Código malicioso capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá por meio da exploração de vulnerabilidades existentes ou falhas na configuração de programas instalados em computadores [4].

[2]Ransomware é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (ransom) para restabelecer o acesso ao usuário [4].

de pagamento [8]; demonstram que o cenário de guerra cibernética já é uma realidade, inspiram uma sensação geral de insegurança e demandam respostas à altura.

Em 2017, os incidentes em massa de fraude ou roubo de dados estão entre os cinco eventos com maior probabilidade, segundo o relatório do Fórum Econômico Mundial intitulado The Global Risks Report 2017 [9]. O mesmo estudo aponta, na categoria de Riscos Tecnológicos, quatro riscos globais[3] relevantes: as consequências adversas dos avanços tecnológicos; os ataques cibernéticos em larga escala; a disrupção de redes computacionais e infraestruturas críticas de informação; e os incidentes massivos de fraude ou roubo de dados. Por fim, dentre as tendências[4] apontadas no estudo, encontra-se o crescimento da ciber-dependência, ou seja, um mundo cada vez mais dependente da tecnologia.

O Livro Verde de Segurança Cibernética [1], estudo publicado no âmbito do GSI, conclui que o entendimento sobre a importância da segurança cibernética caracteriza-se cada vez mais como condição *sine qua non* de desenvolvimento, requerendo para tanto, dentre outras ações, a promoção de diálogos e de intercâmbios de ideias, de iniciativas, de dados e informações, de melhores práticas, para a cooperação no tema, no país e entre países.

A Política Nacional de Inteligência, aprovada por meio do Decreto nº 8.793, de 29 de junho de 2016 [10], alerta que o funcionamento de um aparato estatal não pode prescindir da utilização de tecnologias da informação e das comunicações. Afirma, ainda, que o comprometimento da capacidade operacional do Estado e de sistemas computacionais essenciais ao provimento das necessidades básicas da sociedade deve ser preocupação permanente, exigindo constante aperfeiçoamento técnico dos entes públicos responsáveis pela integridade desses sistemas.

Diante de tais desafios, as nações vêm se preparando, urgentemente, para evitar ou minimizar ataques cibernéticos às redes e sistemas de informação de governo, bem como de todos os demais segmentos da sociedade [1].

Não bastasse toda a complexidade envolvida em ameaças implementadas em software, a constatação da possibilidade de modificações maliciosas no nível do circuito integrado (hardware Trojans, HT) traz novas preocupações.

Embora a questão dos hardware Trojans venha sendo amplamente discutida no mundo, no Brasil pouco se tem falado sobre o tema. Mesmo após as revelações de Edward Snowden sobre as supostas ações de espionagem conduzidas pela agência americana NSA (National Security Agency ou Agência de Segurança Nacional) em setores importantes do Estado

[3]Segundo o relatório, um risco global é definido como um evento ou condição incerta que, se ocorre, pode causar impactos significantes ou negativos em diversos países ou indústrias nos próximos dez anos.

[4]Segundo o estudo, uma tendência é definida como um padrão de longo prazo que está em evolução e que pode contribuir para a ampliação dos riscos globais ou alterar a relação entre eles.

brasileiro, o que se viu foram ações pontuais com foco na espionagem cibernética por meio do comprometimento de software ou dos meios de comunicação.

As respostas normativas ao caso Snowden, a exemplo do Decreto 8.135, de 4 de novembro de 2013 [11], também não endereçaram o tema de forma direta.

Soma-se ainda o fato de que, no Brasil, mesmo que se tenha observado algum avanço nos últimos anos, a indústria doméstica de circuitos integrados permanece inexpressiva e carente de investimentos, posicionando o país como uma nação dependente da tecnologia externa.

Recentemente, o Gabinete de Segurança Institucional (GSI) da Presidência da República (PR), área federal responsável pela coordenação das ações de segurança da informação no Governo, publicou a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018 [12], o que demonstra a vontade do Estado brasileiro em equacionar os problemas afetos à área cibernética, por meio do planejamento e da coordenação de esforços dos órgãos públicos, em parceria com a sociedade.

O documento indicou ainda que, no cenário atual, as ameaças cibernéticas são crescentes, diferenciadas e apresentam elevado grau de sofisticação, exigindo dos governos ações efetivas de prevenção e combate às práticas maliciosas no uso da tecnologia da informação e comunicação, por meio de ações transversais, integradoras, interdisciplinares e multissetoriais.

O momento, portanto, é oportuno para avançar na discussão, que deveria também abordar as questões associadas à ameaça do hardware Trojan.

1.2 Panorama da Indústria de Semicondutores

A indústria de semicondutores desempenha um papel cada vez mais relevante na sociedade atual, fornecendo componentes de microeletrônica utilizados nas mais variadas aplicações digitais [13]. Trata-se de uma indústria caracterizada pelo uso intensivo de tecnologia como vantagem competitiva, sendo um setor altamente lucrativo [14].

A indústria de semicondutores é uma das mais relevantes e dinâmicas no mundo de hoje, e os semicondutores estão no âmago não apenas da Era da Informação e da Comunicação, como também da Indústria 4.0, também conhecida como a Revolução da Internet das Coisas[5] [16].

A indústria mundial de semicondutores caracteriza-se por sua rápida evolução tecnológica, sendo dominada por grandes empresas, que controlam parcela significativa do

[5] A Internet da Coisas pode ser entendida como uma infraestrutura global para a sociedade da informação que permite serviços avançados de interconexão (física e virtual) de coisas ou objetos com base em informação interoperável e tecnologias da informação já existentes ou em evolução [15].

mercado. Em termos de distribuição geográfica, algo em torno de 50% do mercado é atendido por empresas norte-americanas, mas somente 14% da capacidade instalada está nos EUA. Por outro lado, Taiwan e Coreia do Sul lideram em capacidade instalada com mais de 20% cada [16].

Em 2015, o mercado global de semicondutores movimentou algo em torno de US$ 335 bilhões [17], contra US$ 333 bilhões em 2014 e US$ 303 bilhões em 2013 [18].

No Brasil, o setor doméstico ainda é incipiente. A necessidade de o País dispor, em bases competitivas e inovadoras, de uma indústria de semicondutores, é tema exaustivamente debatido dentro do Governo Brasileiro, da academia e da indústria [17].

O sucesso obtido com a fabricação, no País, de diversos equipamentos, tendo por base a Lei de Informática[6] e os incentivos oferecidos pelo Polo Industrial de Manaus[7], não foram suficientes para manter e desenvolver no Brasil a indústria de componentes. No final da década de 80, havia cerca de 23 empresas atuando no setor, mas atualmente a produção nacional de componentes é reduzida e mais voltada ao mercado interno [17].

Ao longo dos últimos 15 anos, uma ampla política de incentivos à indústria de semicondutores foi construída no Brasil. Esta política conta com vários instrumentos, inclusive o maior incentivo fiscal concedido a um setor industrial no Brasil[8]. Ainda assim, tais políticas não são tão agressivas como aquelas que tem sido praticadas em países industrializados [16].

Deste conjunto de instrumentos, o Programa de Apoio ao Desenvolvimento Tecnológico da Indústria de Semicondutores (PADIS) parece ser o mais relevante [16]. O programa foi instituído por meio da Lei nº 11.484, de 31 de maio de 2007 e estabelece que para as empresas que invistam em pesquisa e desenvolvimento no Brasil, e exerçam pelo menos uma das atividades de concepção, desenvolvimento e projeto (*design*), difusão ou processamento físico químico, corte, encapsulamento e testes de semicondutores ou de *displays*, será concedida a desoneração dos impostos e tributos federais incidentes sobre as máquinas, equipamentos e ferramentas destinadas ao projeto e à produção de semicondutores e de *displays* [17].

As principais características do PADIS [19] são:

- A Empresa precisa ser exclusivamente dedicada à produção de bens incentivados pelo Programa (CNPJ exclusivo para o PADIS);
- Submissão prévia de Projeto de P&D e Produção ao MCTI e ao MDIC, segundo roteiro específico;

[6]Lei nº 8.248, de 23 de outubro de 1991

[7]Decreto-Lei nº 288, de 28 de fevereiro de 1967

[8]Segundo o Relatório de Incentivos do Programa PADIS, a renúncia fiscal do programa foi da ordem de R$ 399 milhões em 2015

- Habilitação junto à Receita Federal após a aprovação do projeto;
- Investimento mínimo anual em P&D (3% de 2014 a 2015, 4% de 2016 a 2018 e, a partir de 2019, retorno ao percentual original de 5%, sempre tendo como base de cálculo o faturamento líquido no mercado interno);
- Realização no Brasil das etapas produtivas previstas na legislação.

Até 31 de dezembro de 2015[9], estavam beneficiadas pelo PADIS oito empresas: duas de processamento de lâminas ou *foundries* - CEITEC S.A.[10] (*design* e *foundry*) e Companhia Brasileira de Semicondutores[11] (CBS); duas empresas fabricantes de memórias (DRAM E FLASH) - Smart[12] e HT Micron[13]; três empresas de projeto de circuitos integrados - IC *design houses* - SiliconReef, Chipus[14] e Idea e a empresa FlexIC, fabricante de circuitos híbridos [17].

A Figura 1.1, extraída do Relatório de Incentivos do PADIS no Triênio 2013/2015 [17], publicado pelo Ministério da Ciência, Tecnologia, Inovações e Comunicações, traz a distribuição espacial da indústria de semicondutores no Brasil.

Figura 1.1: Localização da Indústria de Semicondutores no Brasil.

[9]Os relatórios do PADIS são trienais, conforme art. 22 da Lei nº 11.484/2007. O presente relatório abrange o período de 2013 a 2015

[10]www.ceitec-sa.com

[11]www.cbs-semi.com

[12]www.smartm.com

[13]www.htmicron.com.br

[14]www.chipus-ip.com/

Importante ressaltar ainda as instituições credenciadas pelo MCTIC, que realizaram convênios com as empresas beneficiárias do Programa PADIS, para realizarem atividades de pesquisa e desenvolvimento em semicondutores, conforme abaixo [17]:

- Associação do Laboratório de Sistemas Integráveis Tecnológico – LSI-TEC;
- Centro de Pesquisa e Desenvolvimento em Telecomunicações - CPqD
- Centro de Tecnologia da Informação Renato Archer - CTI
- Instituto de Pesquisas Eldorado
- Universidade Federal de Santa Maria - UFSM
- Universidade Federal do Rio Grande do Sul - UFRGS
- Universidade do Vale do Rio dos Sinos - UNISINOS

Em suma, não obstante os avanços conseguidos com as políticas de governo, o setor de semicondutores ainda carece de melhorias no Brasil. Conforme pontuou Filippin [16], a política para a indústria de semicondutores ainda pode ser melhorada em diversos pontos, e talvez o avanço mais importante seja uma melhor articulação dos instrumentos existentes. Também é desejável que o setor volte a ter o reconhecimento estratégico que teve no passado.

1.3 Problema de Pesquisa

Na atualidade os *chips* eletrônicos (circuitos integrados ou CIs) estão presentes em uma infinidade de equipamentos eletrônicos, tais como computadores, notebooks, celulares, *tablets*, em equipamentos médicos, em automóveis, dentre outros, que por sua vez são empregados nas mais diversas áreas, a exemplo das comunicações, das infraestruturas energéticas, dos meios de transporte, dos mercados financeiros, nos sistemas de controle de tráfego aéreo e em muitos outros.

Os CIs concentram boa parte da "inteligência" dos equipamentos, o que faz com que qualquer mal funcionamento nesses pequenos dispositivos afete de forma relevante a confiabilidade da máquina. Considerando que comumente os ataques por código malicioso (vírus de computador e *malwares* em geral) são implementados no nível do software, o hardware, *"the root of trust"* [20] [21] (raiz de confiança), é geralmente considerado a parte do sistema cuja confiança é uma premissa [22] [23]. Até recentemente, essa era uma assunção razoável [24] (Figura 1.2, adaptada de Iqbal [25]).

A possibilidade de implementação de códigos maliciosos no nível do hardware – os chamados *"hardware Trojans"* (HTs) - vem sendo estudada e discutida há alguns anos. A

Figura 1.2: Visão esquemática das tradicionais camadas de ataque cibernético.

globalização da cadeia de suprimentos de CIs e o aumento da complexidade na fabricação desses dispositivos têm incentivado os debates acerca dos problemas de se garantir a confiança no nível do hardware e sobre os riscos decorrentes da perda de controle sobre os processos presentes na cadeia de suprimentos de CIs. Estudos revelam a possibilidade de CIs serem "intencionalmente comprometidos durante o processo de design, antes mesmo de serem manufaturados" [26]. Ou ainda, a alteração pode se dar durante o processo de manufatura [20]. As possibilidades são diversas e potencialmente envolvem comprometimentos na disponibilidade, na integridade e na confidencialidade de dados que trafegam no hardware.

HTs podem lançar ataques com efeitos graves, como a desativação ou alteração da funcionalidade de um CI, ou o vazamento de informações confidenciais do usuário [27]. Não obstante, os HTs não são necessariamente implementados objetivando-se um ataque específico e imediato, mas podem apenas "suportar ataques" [28], a serem lançados por meio de um gatilho (*trigger*) acionado *a posteriori*. Essa possibilidade permitiria uma espécie de infiltração silenciosa na cadeia de suprimentos, dando ao atacante a oportunidade de lançar, em momento oportuno, um "ataque de hardware em larga escala" [29].

Não obstante os riscos e danos em potencial, a detecção do HT não é um tarefa simples, e as técnicas existentes atualmente não são efetivas o bastante [22] para detectá-lo. O ex-chefe da CIA e NSA, General Michael Hayden, chegou a declarar que a questão de hardware comprometido é um problema que não pode ser resolvido, mas uma situação que deve ser gerenciada [30].

Portanto, entender a ameaça e criar capacidade de reação é uma necessidade, e estudos futuros terão que focar na combinação das melhores técnicas de prevenção e detecção para

prover equipamentos livres da ameaça do HT [31].

1.4 Motivação

Os estudos sobre o fenômeno hardware Trojan são relativamente recentes no mundo, e no Brasil são ainda incipientes.

Assim, dentre as motivações do presente estudo, destaca-se a importância de se alertar o país pra a existência do problema, sensibilizando áreas do governo federal responsáveis pela segurança da informação e segurança cibernética, além de buscar um posicionamento do país no contexto da pesquisa mundial, que vem crescendo em estudos sobre a temática do hardware Trojan e suas implementações maliciosas nos CIs.

Dotar o país de mecanismos que permitam uma defesa completa em relação a tais ameaças não é um caminho simples, como se verá ao longo do estudo. Mas é importante que o país esteja ciente sobre o fenômeno e suas implicações, e possa, no presente, tomar ações que produzam resultados no curto, médio e longo prazo.

Portanto, a importância de se contribuir para a pesquisa na área de segurança cibernética no país, permitindo que pesquisadores e profissionais atuantes na área possam se valer de um arcabouço teórico e propositivo, eventualmente expandindo e extrapolando os conhecimentos no tema é, em essência, o grande motivador do presente estudo.

1.5 Objetivos

1.5.1 Objetivo Geral

Proposição de desdobramentos no nível tático dos Objetivos Estratégicos definidos na Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal.

1.5.2 Objetivos específicos

O objetivo geral se desdobra nos seguintes objetivos específicos:

1. Pesquisar as ameaças do hardware Trojan;
2. Analisar as implicações do hardware Trojan no contexto da segurança da informação e da segurança cibernética;
3. Identificar as implicações do fenômeno hardware Trojan em questões relativas à segurança cibernética brasileira;

1.6 Limitações

No caso em estudo, primeiramente houve o estabelecimento de um limite temporal. Na revisão bibliográfica, particularmente após a aplicação do enfoque meta-analítico, observou-se que as produções acadêmicas sobre a temática do hardware Trojan eram raras ou inexistentes antes do ano de 2007. Assim, foi estabelecido o horizonte temporal de 11 anos para a pesquisa bibliográfica, cobrindo o período de 2007 a 2017.

Ainda sobre a revisão bibliográfica, o presente trabalho não objetivou exaurir as várias formas de implementação e detecção do HT, mas apresentá-las de forma geral, tratando alguns casos considerados relevantes.

Sobre a abordagem do tema, tem-se que o assunto envolve questões sobre segurança da informação e segurança cibernética, conforme será exposto no Capítulo 4. No entanto, a pesquisa concentrou sua atenção na segurança cibernética, sopesando, em essência, dois aspectos principais: a proximidade do conceito com a temática do hardware Trojan, dado que a segurança cibernética envolve o conceito de ativos de informação, alvos, por excelência, da ameaça dos HT; e o fato de que a segurança da informação e comunicações tem escopo bem mais amplo, abarcando inclusive a própria segurança cibernética.

Conforme será exposto no Capítulo 4, o tema hardware Trojan envolve questões de espionagem e soberania entre países.

É fato que órgãos de inteligência são caracterizados pela discrição e pela salvaguarda de informações. Nos termos da Lei nº 9.883/1999 [32], compete à Agência Brasileira de Inteligência (ABIN), órgão central do Sistema Brasileiro de Inteligência (SISBIN), planejar e executar a proteção de conhecimentos sensíveis, relativos aos interesses e à segurança do Estado e da sociedade, dentre outras atribuições.

Devido a essa característica peculiar do tema em estudo, houve limitações, durante a pesquisa, em relação ao acesso a determinadas informações consideradas sensíveis pelos órgãos envolvidos com a temática. Assim, a presente pesquisa fez uso, em essência, de informações públicas, obtidas através de instrumentos legais, normativos, leis, decretos, instruções normativas, sítios de internet, planos, estratégias, documentos oficiais publicados por órgãos governamentais, dentre outros, além de livros, teses e artigos produzidos no meio acadêmico.

Portanto, as análises, proposições e conclusões trazidas no âmbito da pesquisa foram elaboradas sob essas limitações.

1.7 Estrutura do Trabalho

O presente trabalho foi estruturado em 6 capítulos, que serão brevemente descritos a seguir.

- No Capítulo 1, Introdução, faz-se a contextualização do problema na seção 1.1. Um breve panorama da indústria de semicondutores é apresentado na seção 1.2. O problema de pesquisa é detalhado em 1.3. As motivações que levaram o autor a investigar o tema de pesquisa são detalhadas na seção 1.4. A seguir, na seção 1.5, os objetivos gerais e específicos são apresentados. E, por fim, na seção 1.6, as limitações da pesquisa são esclarecidas.
- No Capítulo 2, Revisão da Literatura, são apresentados na seção 2.1 todos os resultados do levantamento bibliográfico por meio da utilização do enfoque meta-analítico. A seguir, na seção 2.2, faz-se uma revisão abrangente de todos os conceitos envolvidos na temática principal da pesquisa, o hardware Trojan (HT). Conceitos fundamentais são apresentados; a taxonomia é analisada; e, por fim, pontos de inserção, implementações e técnicas de detecção do HT são descritos. No item 2.3, aborda-se sobre o hardware Trojan e suas implicações no contexto da segurança da informação e da segurança cibernética. No tópico a seguir (2.4), discorre-se sobre o planejamento estratégico, tático e operacional, abordando inclusive as metodologias BSC e 5W2H.
- O Capítulo 3, Metodologia, apresenta as etapas metodológicas utilizadas pelo autor na elaboração da pesquisa, que objetivaram o atingimento dos objetivos propostos.
- O Capítulo 4 envolve a Pesquisa Documental. Na seção 4.1, apresenta-se descritivo sobre os órgãos da Administração Pública Federal no contexto da segurança da informação e da segurança cibernética. A seguir, na seção 4.2, analisa-se as implicações do fenômeno hardware Trojan em questões relativas à segurança cibernética brasileira. Por fim, na seção 4.3, faz-se um resumo conciso da Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015 - 2018, documento publicado pelo Gabinete de Segurança Institucional da Presidência da República.
- No Capítulo 5, Elaboração de Propostas, apresentam-se propostas de desdobramentos táticos dos Objetivos Estratégicos definidos na Estratégia de SIC e de SegCiber.
- Por fim, o Capítulo 6 dedica-se a apresentar as conclusões do estudo e as evidências de que os objetivos propostos foram atingidos, bem como sugestões para trabalhos futuros.

Capítulo 2

Revisão da Literatura

2.1 Levantamento bibliográfico e resultados do enfoque meta-analítico

Conforme apresentado anteriormente, o presente trabalho utilizou a pesquisa bibliográfica de caráter exploratório e descritivo por meio do enfoque meta-analítico, método de sete fases conforme proposto por Mariano [33], em adaptação ao estudo de Garcia e Ramirez [34].

Para a aplicação do enfoque meta-analítico, este trabalho utilizou a base de dados dos repositórios ISI Web of Science [1] e Scopus [2], no período de 2007 a 2017. Segundo Chadegani *et al* [35], as bases Scopus e Web of Science respondem pelos maiores bancos de dados de artigos utilizados pela comunidade científica mundial.

Uso da base ISI Web of Science: De acordo com o enfoque meta-analítico, a primeira fase consiste no levantamento de revistas relativas à disciplina estudada [33]. Para a escolha das revistas nesses portais, é necessário selecionar categorias temáticas afetas à área de conhecimento pesquisada. As categorias temáticas (áreas de conhecimento) identificadas no portal Web of Science que guardam alguma afinidade com o tema dessa dissertação foram as seguintes:

- *Automation Control Systems* (Sistemas de Controle de Automação);
- *Computer Science, Artificial Intelligence* (Ciência da Computação, Inteligência Artificial);
- *Computer Science, Cybernetics* (Ciência da Computação, Cibernética);

[1] www.webofknowledge.com
[2] www.scopus.com

- *Computer Science, Hardware and Architecture* (Ciência da Computação, Hardware e Arquitetura);
- *Computer Science, Information Systems* (Ciência da Computação, Sistemas de Informação);
- *Computer Science, Interdisciplinary Applications* (Ciência da Computação, Aplicações Interdisciplinares);
- *Computer Science, Software Engineering* (Ciência da Computação, Engenharia de Software);
- *Computer Science, Theory Methods* (Métodos Teóricos);
- *Engineering, Electrical and Electronic* (Engenharia, Elétrica e Eletrônica);
- *Engineering, Industrial* (Engenharia, Industrial);
- *Engineering, Manufacturing* (Engenharia, Produção);
- *Telecommunications* (Telecomunicações).

Após a identificação do universo de revistas afetas ao tema em estudo, procura-se, na segunda fase, elaborar um ranking das revistas mais relevantes, de acordo com critérios bem definidos. A ferramenta utilizada foi o Journal Citation Reports (JCR) do portal Web of Science, que é um módulo do portal utilizado para a geração de relatórios de citações de revistas. O ranking baseou-se no indicador Journal Impact Factor (JIF). Conforme definição obtida no glossário disponibilizado pelo próprio site, o JIF contempla todas as citações à revista no ano atual do JCR para os itens publicados nos dois anos anteriores, dividido pelo número total de artigos acadêmicos (artigos, resenhas e artigos de trabalhos) publicados na revista nos dois anos anteriores. O ano de referência (mais recente) disponível no site, no momento desta pesquisa, é 2016 (Journal Citation Reports Year).

A Tabela 2.1 (extraída da base Web of Science, acesso em 18/11/2017) apresenta o ranking das dez primeiras revistas classificadas por JIF:

Na terceira fase – "preencher base de dados com artigos", realiza-se pesquisa sobre o tema utilizando como filtro as palavras chaves do estudo e as publicações selecionadas anteriormente [33], de forma a obter uma lista de artigos que versam sobre o tema em análise. No caso em estudo, foram utilizadas as seguintes palavras-chave: Hardware Trojan; Trojan Circuit; Silicon Trojan; e Malicious Circuit.

Ao fazer essa busca, é importante a delimitação temporal. No caso em estudo, utilizou-se o horizonte de 11 anos (2007 a 2017). Os motivos dessa limitação foram expostos no Capítulo 1 (Limitações).

Tabela 2.1: Ranking das 10 primeiras revistas por JIF

Rank	**Título**	**Total de Citações**	**Fator de Impacto (JIF)**
1	IEEE Communications Surveys and Tutorials	8.654	17,188
2	Progress in Quantum Electronics	1.047	11,000
3	IEEE Industrial Electronics Magazine	1.119	10,710
4	IEEE Transactions on Evolutionary Computation	11.006	10,629
5	IEEE Comunications Magazine	17.250	10,435
6	IEEE signal processing magazine	9.088	9,654
7	Journal of Statistical Software	10.301	9,436
8	Proceedings of the IEEE	30.230	9,237
9	IEEE Wireless Comunications	5.479	8,972
10	IEEE Transactions on Pattern Analysis and Machine Intelligence	43.649	8,329

Sobre a pesquisa de artigos na base WOS, apenas a palavra-chave "Hardware Trojan"resultou em quantidade relevante de documentos (351 artigos), o que mostra que a expressão é a mais usada para tratar sobre o tema. As demais expressões resultaram em 25 artigos ("Trojan Circuit"), nenhum artigo ("Silicon Trojan") e 13 artigos ("Malicious Circuit"). Por essa razão, as fases do enfoque meta analítico serão aplicadas apenas no tema "Hardware Trojan".

Dentre as revistas ou conferências que mais publicaram trabalhos sobre o tema "hardware Trojan", destacam-se (Tabela 2.2, retirada do portal Web of Science, acesso em 18/11/2017):

A análise a seguir (Figura 2.1, retirada do portal Web of Science, acesso em 18/11/2017) traz uma visão sobre a evolução da temática ao longo do tempo, indicando o número de artigos publicados anualmente sobre o tema "hardware Trojan".

Observa-se uma evolução contínua do tema ao longo da última década, cuja publicação era rara no início da série (apenas 1 publicação em 2007 e 7 publicações em 2008), apresentando evolução rápida a partir de 2013, com pico de publicações no ano de 2015 (88 publicações).

A seguir, temos a análise por país de publicação (Figura 2.2, retirada de Web of Science, acesso em 18/11/2017):

Observa-se claramente que as universidades norte-americanas vem mantendo a liderança em publicações sobre o tema HT, embora China, Índia e França também apresentem número relevante de pesquisas sobre o tema.

Tabela 2.2: Base Web of Science: revistas que mais publicaram artigos sobre o tema hardware Trojan

Rank	Título da fonte	Registros	% of 351
1	Design Automation and Test in Europe Conference and Exhibition	12	3,419
2	IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems	11	3,134
3	ICCAD IEEE ACM International Conference on Computer Aided Design	9	2,564
4	IEEE Transactions on Information Forensics and Security	9	2,564
5	Design Automation Conference DAC	8	2,279
6	Journal of Electronic Testing Theory and Applications	7	1,994
7	Lecture Notes in Computer Science	7	1,994
8	Midwest Symposium on Circuits and Systems Conference Proceedings	7	1,994
9	2015 IEEE International Symposium on Hardware Oriented Security and Trust Host	6	1,709
10	IEEE International Symposium on Circuits and Systems	6	1,709

E, finalmente, a análise sobre o número de citações do tema, por ano (Figura 2.3, retirada de Web of Science, acesso em 18/11/2017).

Da análise comparativa entre a Figura 2.3 e a Figura 2.1, observa-se que há uma coerência entre o crescimento do número de publicações sobre o tema HT e o crescimento do número de citações, o que demonstra que as pesquisas e o interesse sobre o tema vem avançando na comunidade acadêmica.

Na quarta etapa, procede-se a análise de autores e artigos. Segundo Mariano [33], esta fase é dividida em duas partes: análise do número de artigos por autor (análise quantitativa); e análise dos autores mais citados (análise qualitativa).

A seguir (Tabela 2.3, retirada de Web of Science, acesso em 18/11/2017) são apresentados os 15 autores com mais artigos sobre o tema:

Mohammad Tehranipoor (University of Florida); Swarup Bhunia (University of Florida); Rajat Subhra Chakraborty (Indian Institute of Technology Kharagpur); e Domenic Forte (University of Florida), lideram o ranking com cerca de 20% de todas as publicações sobre o tema HT na base Web of Science.

A tabela a seguir (Tabela 2.4, retirada de Web of Science, acesso em 18/11/2017) classifica os 10 primeiros artigos conforme o número de citações.

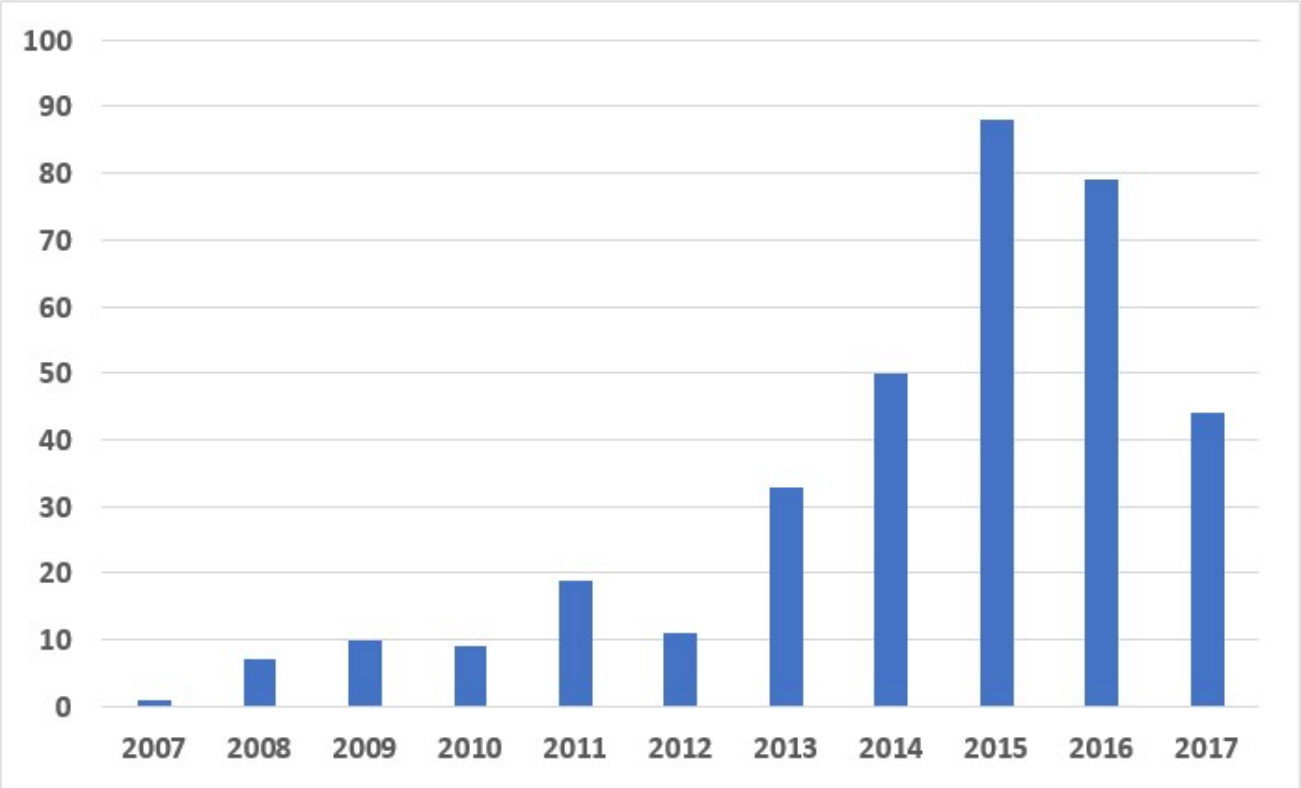

Figura 2.1: Itens publicados por ano sobre o tema hardware Trojan.

Tabela 2.3: Autores com mais artigos sobre o tema hardware Trojan

Rank	Autores	Registros	% de 351
1	Tehranipoor M	26	7,407
2	Bhunia S	19	5,413
3	Chakraborty RS	15	4,274
4	Forte D	11	3,134
5	Plusquellic J	11	3,134
6	Hasan SR	9	2,564
7	Jin Y	9	2,564
8	Potkonjak M	9	2,564
9	Salmani H	9	2,564
10	Bhasin S	8	2,279
11	Guilley S	8	2,279
12	Koushanfar F	8	2,279
13	Makris Y	8	2,279
14	Wang LW	8	2,279
15	Danger JL	7	1,994

Na quinta etapa, determina-se linhas e enfoques teóricos de pesquisa a partir da análise dos principais artigos e de seus posicionamentos [33].

Campo: Países/Territórios	Contagem do registro	% de 351	Gráfico de barras
USA	164	46.724 %	
PEOPLES R CHINA	69	19.658 %	
INDIA	37	10.541 %	
FRANCE	29	8.262 %	
JAPAN	13	3.704 %	
SINGAPORE	13	3.704 %	
EGYPT	10	2.849 %	
IRAN	10	2.849 %	
AUSTRIA	9	2.564 %	
U ARAB EMIRATES	9	2.564 %	

Figura 2.2: Publicações sobre o tema hardware Trojan, por país.

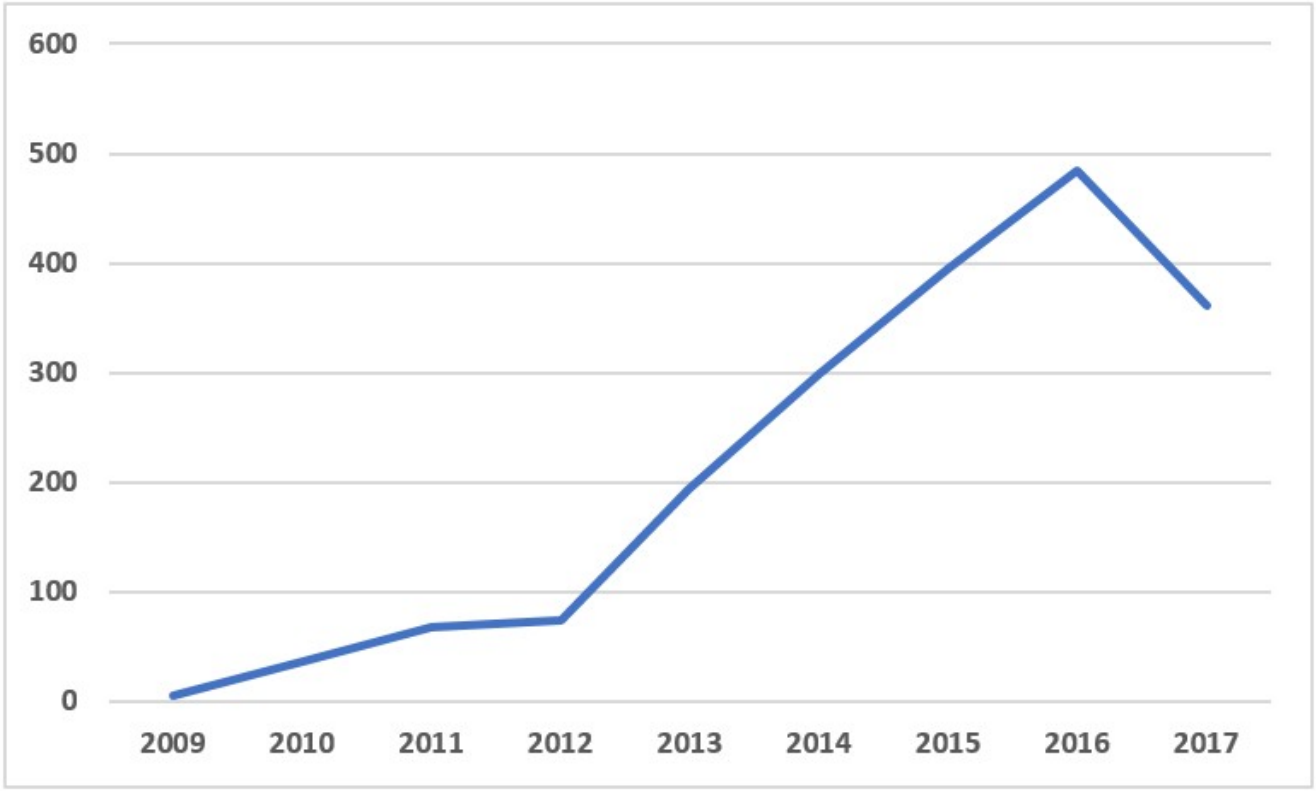

Figura 2.3: Citações sobre o tema hardware Trojan a cada ano.

Dos principais artigos elencados na base (artigos com mais citações conforme Tabela 2.4), observa-se claramente que o enfoque da detecção do HT é o mais relevante,

Tabela 2.4: Artigos sobre o tema hardware Trojan com maior número de citações

Rank	Artigo	Autores	Citações
1	A Survey of Hardware Trojan Taxonomy and Detection	Tehranipoor, Mohammad; Koushanfar, Farinaz	241
2	Hardware Trojan detection using path delay fingerprint	Jin, Yier; Makris, Yiorgos	152
3	Trustworthy Hardware: Identifying and Classifying Hardware Trojans	Karri, Ramesh; Rajendran, Jeyavijayan; Rosenfeld, Kurt; Tehranipoor, Mohammad	109
4	Hardware Trojan Horse Detection Using Gate-Level Characterization	Potkonjak, Miodrag; Nahapetian, Ani; Nelson, Michael; Massey, Tammara	76
5	At-speed delay characterization for IC authentication and Trojan Horse detection	Li, Jie; Lach, John	73
6	Hardware Trojan: Threats and Emerging Solutions	Chakraborty, Rajat Subhra; Narasimhan, Seetharam; Bhunia, Swarup	63
7	Hardware Trojan Attacks: Threat Analysis and Countermeasures	Bhunia, Swarup; Hsiao, Michael S.; Banga, Mainak; Narasimhan, Seetharam	62
8	A Novel Technique for Improving Hardware Trojan Detection and Reducing Trojan Activation Time	Salmani, Hassan; Tehranipoor, Mohammad; Plusquellic, Jim	57
9	MERO: A Statistical Approach for Hardware Trojan Detection	Chakraborty, Rajat Subhra; Wolff, Francis; Paul, Somnath; Papachristou, Christos; Bhunia, Swarup	53
10	Hardware Trojan Detection and Isolation Using Current Integration and Localized Current Analysis	Wang, Xiaoxiao; Salmani, Hassan; Tehranipoor, Mohammad; et al.	52

responsável por cerca de 766 das 938 citações entre os dez primeiros artigos.

O segundo enfoque mais comum recai sobre classificações e taxonomias, que totalizam em torno de 475 de 938 citações. Cabe ressaltar que diversos artigos abordaram, simultaneamente, os dois temas.

O resultado parece-nos esperado. Como será visto mais adiante, a detecção do HT é extremamente complexa, o que vem se apresentando como um grande desafio no tratamento dessa ameaça. E, por outro lado, os esforços de classificação e taxonomia buscam uma compreensão mas ampla sobre o fenômeno, preparando o terreno para possíveis soluções.

A sexta etapa envolve a análise das palavras chaves (*keywords*) presentes nos artigos

estudados. Estas palavras revelam características próprias de cada trabalho, permitindo agrupar os estudos e classifica-los [33]. A partir da base de artigos, extrai-se somente as palavras-chaves para que se proceda a análise pretendida. O uso de ferramentas de "*word cloud*", ou nuvem de palavras, pode facilitar a visualização de palavras e respectivas frequências. Tais ferramentas dispõe graficamente diversas palavras lidas de uma fonte, categorizando-as de acordo com a frequência em que ocorram (maior a frequência, maior é o tamanho da fonte). Na figura abaixo (Figura 2.4), utilizou-se a ferramenta "TagCrowd" [3].

Figura 2.4: Nuvem de palavras - artigos sobre tema hardware Trojan.

Destacam-se como palavras-chaves de maior incidência: *hardware; trojan; security; circuit; analysis;* e *detection.*

As duas primeiras formam o termo utilizado nesse estudo (hardware Trojan), e seria esperado sua aparição com maior frequência. "*Security*", "*analysis*"e "*circuit*"guardam afinidade com exposições conceituais sobre o tema. Destaca-se, por fim, a palavra "*detection*", que evidencia, de forma coerente, o principal enfoque teórico apontado na quinta etapa da meta-análise.

Na última etapa, procura-se realizar um estudo das relações existentes entre os artigos previamente selecionados nas fases anteriores.

É importante investigar quais enfoques foram mais abordados, como têm sido elaboradas as pesquisas (laboratório ou em campo), qual a população/amostra/participantes, entre outras informações [36].

A Tabela 2.5 apresenta, de forma sintética, alguns dos principais autores sobre o tema, artigos relevantes e enfoques abordados.

[3] tagcrowd.com

Tabela 2.5: Estudo das Relações

Autor	Artigo	Enfoque
Tehranipoor, Mohammad	A survey of hardware trojan taxonomy and detection	Apresenta uma classificação para os hardware Trojans e analisa as principais pesquisas sobre a detecção da ameaça.
Tehranipoor, Mohammad	A Novel Technique for Improving Hardware Trojan Detection and Reducing Trojan Activation Time	Propõe uma técnica para aprimorar a detecção do HT a partir da redução de seu tempo de ativação.
Tehranipoor, Mohammad	Trustworthy Hardware: identifying and classifying hardware Trojans	Propõe uma taxonomia para o hardware Trojan.
Jin, Yier	Hardware Trojan detection using path delay fingerprint Tehranipoor, Mohammad	Apresenta um método de detecção de HT baseado na identificação de parâmetros de atraso (delay) em chips validados (livres de Trojan), e sua comparação com chips a validar.
Jin, Yier	Experiences in Hardware Trojan Design and Implementation	Aborda experiências de implementação e design de HT realizadas no âmbito de uma competição promovida no Instituto Politécnico de Nova York.
Li, Jie	At-speed delay characterization for IC authentication and TrojanHorse detection	Propõe técnica baseada na medição de parâmetros de atraso (dely) para detectar não só chips falsificados, mas aqueles com possíveis alterações maliciosas (HT).
Chakraborty, Rajat	Hardware Trojan: Threats and Emerging Solutions	Propõe uma taxonomia para o HT e apresenta revisão do estado da arte sobre prevenção e detecção da ameaça.
Bhunia, Swarup	Hardware Trojan Attacks: Threat Analysis and Countermeasures	Apresenta pesquisa sobre o estado da arte em ataques de HT, modelagem e contramedidas.

Da análise precedente, observa-se que a maioria dos autores se utiliza de pesquisa em laboratório, descrevendo e analisando o que potencialmente ocorreria, partindo de ambientes controlados.

De fato, a observação do fenômeno em casos reais permanece um desafio, desde que "ainda não há hardware Trojans reportados na prática" [20].

Uso da base Scopus: As categorias identificadas no portal Scopus que guardam alguma afinidade com o tema dessa dissertação foram as seguintes: *Computer Science* (Ciência da Computação); *Engineering* (Engenharia); *Mathematics* (Matemática); *Materials Science* (Ciência dos Materiais); *Physics and Astronomy* (Física e Astronomia); *Decision Science* (Ciências da Decisão); *Multidisciplinary* (Multidisciplinar); e *Energy* (Energia).

Considerando que os resultados obtidos na base Scopus foram completamente compatíveis com aqueles obtidos na base Web of Science, não acrescentando, portanto, conclusões ou visões novas, apenas serão descritos, de forma sintética, os principais resultados da análise naquela base.

Após a identificação do universo de revistas afetas ao tema em estudo, procura-se elaborar um ranking das revistas mais relevantes. O parâmetro utilizado foi o CiteScore do portal Scopus, que reflete a média de citações recebidas pelo trabalho nos últimos 3 anos. Conforme informação disponibilizada no portal, a metodologia do CiteScore é de 2016 e suas métricas foram calculadas em 31 de maio de 2017[4].

Na Tabela 2.6 (retirada da base Scopus, acesso em 18/11/2017), temos o ranking das 10 primeiras revistas por CiteScore.

Tabela 2.6: Ranking das Revistas

Rank	Título da Revista	CiteScore
1	Reviews of Modern Physics	35,68
2	Annual Review of Astronomy and Astrophysics	35,21
3	Materials Science and Engineering: R: Reports	30,19
4	Progress in Materials Science	30,01
5	Progress in Polymer Science	27,07
6	Energy and Environmental Science	26,39
7	IEEE Communications Surveys and Tutorials	23,80
8	Nature Materials	23,67
9	Foundations and Trends in Signal Processing	23,00
10	Nature Nanotechnology	21,85

O resultado da pesquisa pela palavra-chave "hardware Trojan"encontrou 664 documentos, dentre artigos, conference papers, conference reviews e outros.

Dentre as revistas ou conferências que mais publicaram trabalhos sobre o tema "hardware Trojan", destacam-se (Tabela 2.7, retirada da base Scopus, acesso em 18/11/2017):

A análise a seguir (Figura 2.5, retirada da base Scopus, acesso em 18/11/2017) traz uma visão sobre a evolução da temática ao longo do tempo, indicando o número de artigos publicados anualmente sobre o tema "hardware Trojan".

[4]https://journalmetrics.scopus.com/, acesso em 18/11/2017

Tabela 2.7: Revistas com mais trabalhos divulgados sobre o tema hardware Trojan

	Títulos da fonte	Registros
1	Lecture Notes In Computer Science Including Subseries Lecture Notes In Artificial Intelligence And Lecture Notes In Bioinformatics	23
2	IEEE ACM International Conference On Computer Aided Design Digest Of Technical Papers Iccad	16
3	IEEE Transactions On Computer Aided Design Of Integrated Circuits And Systems	16
4	Proceedings IEEE International Symposium On Circuits And Systems	14
5	Proceedings Of The ACM Great Lakes Symposium On VLSI Glsvlsi	12
6	IEEE Transactions On Information Forensics And Security	11
7	Proceedings IEEE International Conference On Computer Design VLSI In Computers And Processors	9
8	Midwest Symposium On Circuits And Systems	8
9	Journal of Electronic Testing Theory and Applications JETTA	8
10	IEEE Transactions On Very Large Scale Integration VLSI Systems	8

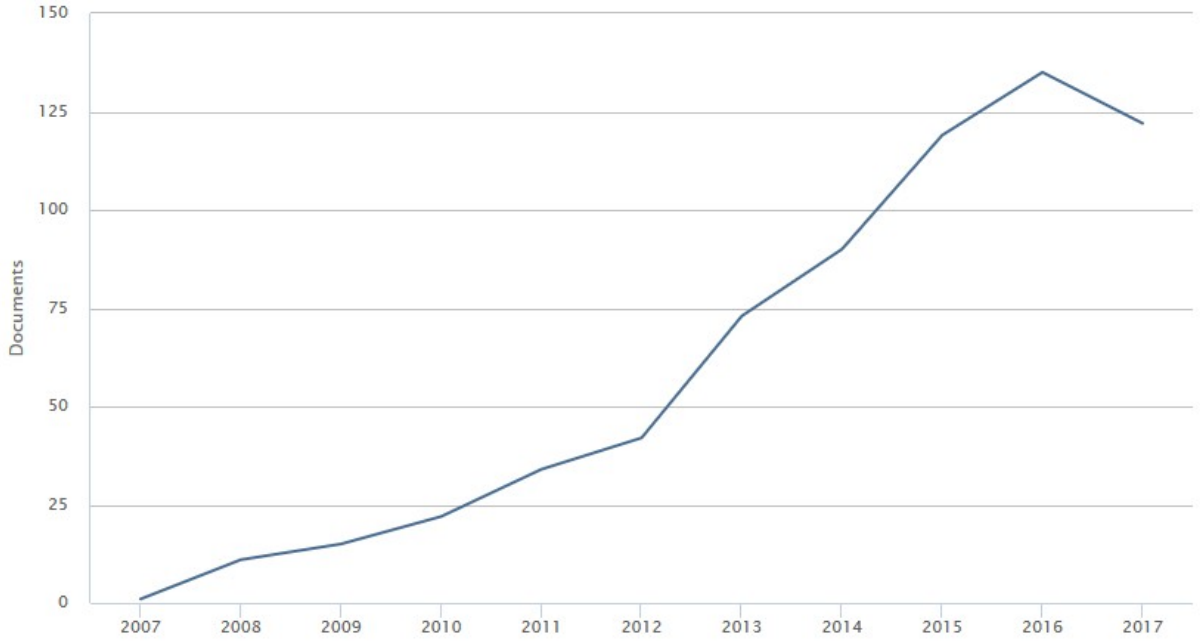

Figura 2.5: Itens publicados por ano sobre o tema hardware Trojan.

Observa-se que a produção de pesquisas em torno do tema hardware Trojan de fato concentra-se na última década, a partir de 2008, com tendência crescente, em especial após o ano de 2012.

A seguir, temos a análise por país de publicação (Figura 2.6, retirada da base Scopus, acesso em 18/11/2017):

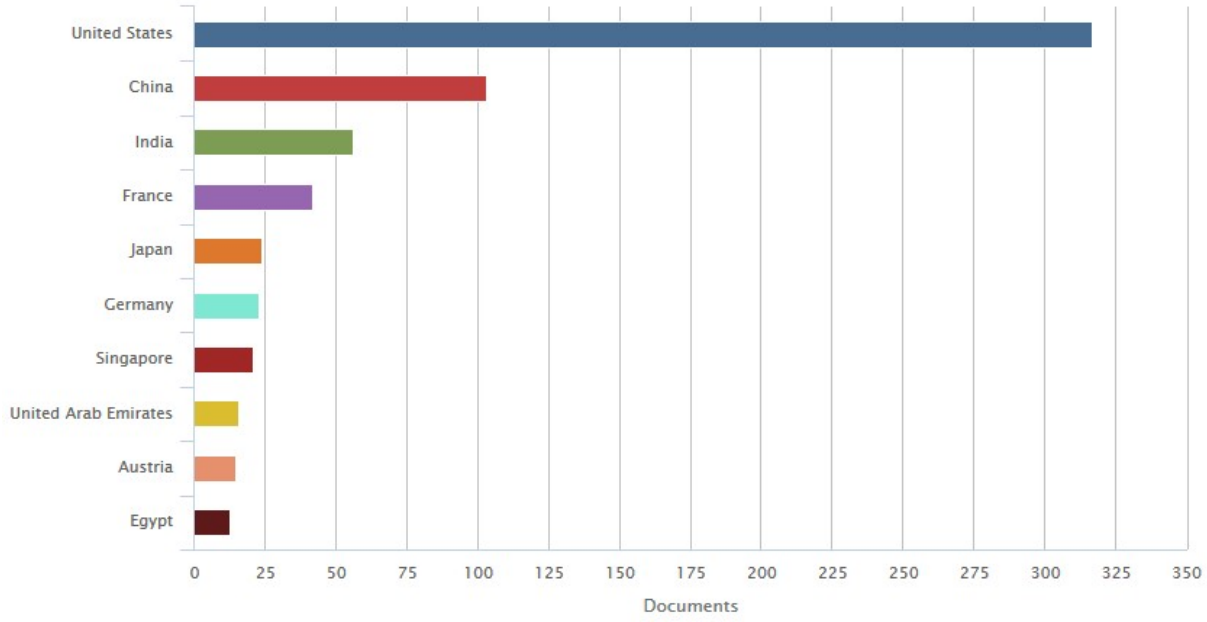

Figura 2.6: Publicações sobre o tema hardware Trojan, por país.

A maior parte das pesquisas sobre a temática HT concentra-se em universidades dos Estados Unidos, que contam com aproximadamente o triplo de artigos publicados em relação ao segundo colocado, a China. Em terceiro, segue a Índia, que recentemente superou a França na produção acadêmica sobre a temática[5].

Finalizando essa etapa, tem-se a análise sobre o número de citações do tema, por ano (Figura 2.7, retirada da base Scopus, acesso em 18/11/2017).

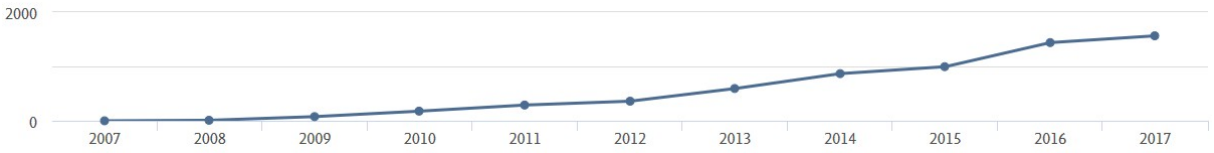

Figura 2.7: Citações sobre o tema hardware Trojan a cada ano.

Da análise das Figuras 2.5 e 2.7, observa-se que o número de citações segue a tendência de incremento em publicações sobre o tema HT, com pouca ou nenhuma citação até 2008, e crescimento acentuado a partir do ano de 2013.

A seguir, apresentamos os autores com mais artigos sobre o tema (Figura 2.8, retirada da base Scopus, acesso em 18/11/2017):

[5]A França figurava em terceiro lugar, seguida pela Índia, em consulta à base Scopus realizada em 12/07/2017

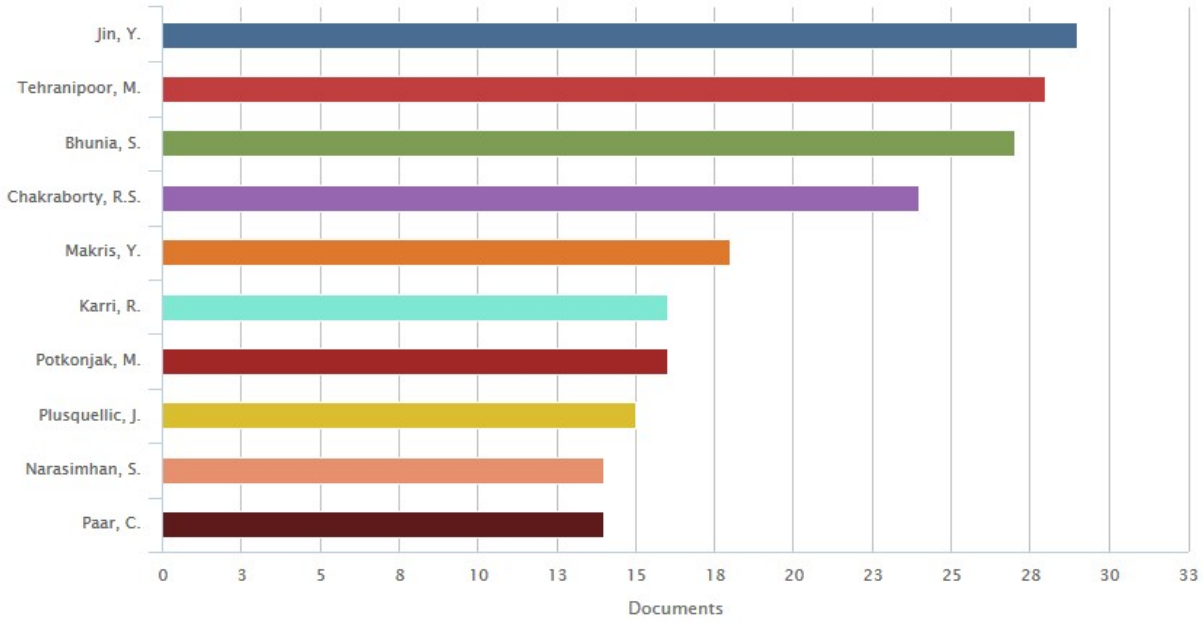

Figura 2.8: Autores com mais artigos sobre o tema.

Yier Jin (University of Florida); Mohammad Tehranipoor (University of Florida); Swarup Bhunia (University of Florida); e Rajat Subhra Chakraborty (Indian Institute of Technology Kharagpur), lideram o ranking com cerca de 16% de todas as publicações sobre o tema HT na base Scopus.

A Tabela 2.8 classifica os 10 primeiros artigos conforme o número de citações.

Terminadas as fases do enfoque meta analítico, o pesquisador poderá trabalhar com os melhores artigos, dos autores mais citados nas revistas com maior impacto, que acompanham as tendências dos estudos sobre um tema em crescimento, buscando a contribuição das melhores linhas de pesquisa e enfoques teóricos [33].

2.2 Hardware Trojan

2.2.1 Circuitos Integrados

Os circuitos integrados (CI) são dispositivos presentes em uma infinidade de equipamentos eletrônicos da atualidade. Eles são constituídos por uma matriz microscópica de circuitos eletrônicos e outros componentes, tais como resistores, capacitores, diodos e transistores, implantados na superfície de um material semicondutor – como o silício, por exemplo [37]. Dessa forma, o circuito resultante é um *chip* monolítico (inteiriço), que pode ser tão pequeno a ponto de ocupar poucos centímetros ou mesmo milímetros quadrados de área.

Tabela 2.8: Artigos sobre o tema hardware Trojan com maior número de citações

	Artigo	Autores	Citações
1	A Survey of Hardware Trojan Taxonomy and Detection	Tehranipoor, Mohammad; Koushanfar, Farinaz	387
2	Hardware Trojan detection using path delay fingerprint	Jin, Yier; Makris, Yiorgos	293
3	Trustworthy Hardware: Identifying and Classifying Hardware Trojans	Karri, Ramesh; Rajendran, Jeyavijayan; Rosenfeld, Kurt; et al.	164
4	At-speed delay characterization for IC authentication and Trojan Horse detection	Li, Jie; Lach, John	148
5	Towards trojan-free trusted ICs: Problem analysis and detection scheme	Li, J., Lach, J.	145
6	Detecting malicious inclusions in secure hardware: Challenges and solutions	Wang, X., Tehranipoor, M., Plusquellic, J.	141
7	Hardware Trojan Horse Detection Using Gate-Level Characterization	Potkonjak, Miodrag; Nahapetian, Ani; Nelson, Michael; et al.	131
8	Hardware Trojan: Threats and Emerging Solutionn	Chakraborty, Rajat Subhra; Narasimhan, Seetharam; Bhunia, Swarup	122
9	A region based approach for the identification of hardware Trojans	Banga, M., Hsiao, M.S.	121
10	Security Analysis of Logic Obfuscation	Rajendran, J., Pino, Y., Sinagoglu, O., Karri, R.	95

Assim, os componentes individuais do circuito geralmente apresentam tamanhos microscópicos [38].

Quando finalizados, os CI são geralmente envoltos em estruturas de plástico que incluem pinos de metal que farão a conexão dos *chips* com o "mundo exterior", como a placa-mãe de um computador [38].

A Figura 2.9, retirada de Floyd [39], traz a representação em corte de um CI típico.

O material semicondutor, sob o qual os CI são implementados, é um tipo de material que pode agir como um condutor ou insulador da eletricidade, a depender de determinadas condições [40]. Assim, semicondutores podem ter a condutividade ampliada a partir da adição de impurezas (outros elementos atômicos) de forma controlada. De forma oposta, áreas do semicondutor com pouca ou nenhuma impureza agirão como insuladoras da eletricidade.

A fabricação de um CI é um processo complexo que chega a envolver, em alguns

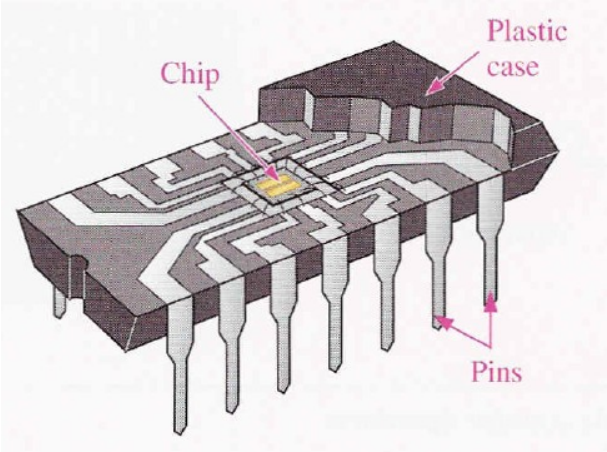

Figura 2.9: Visão em corte de um Circuito Integrado.

casos, mais de quatrocentas etapas [37]. No entanto, visto de uma forma simplificada, pode-se enumerar cinco macroprocessos genéricos, conforme demonstrado na Figura 2.10 (adaptada de Villasenor [26]).

Figura 2.10: Etapas da fabricação de um circuito integrado.

Conforme Villasenor [26], o processo de fabricação de um CI se inicia na especificação, que consiste na definição das funcionalidades do CI, incluindo características como velocidade, capacidade de processamento, dentre outras. Na fase do design, as especificações são então traduzidas na forma de operações lógicas e, posteriormente, nos circuitos elétricos correspondentes. Uma vez finalizado, o projeto de design é então enviado para uma fábrica de semicondutores, onde de fato ocorre a manufatura física do CI. Após, testes de qualidade são feitos em amostras do circuito integrado e só então ele estará pronto para ser inserido em algum equipamento.

Segundo Filippin [16], a produção de um circuito integrado pode ser dividida em 5 etapas: (i) concepção do produto, que pode ou não ser realizada em conjunto com o fabricante do bem final e que é a etapa na qual são definidas as funcionalidades do chip; (ii) projeto ou design do componente; (iii) fabricação do componente; (iv) teste, afinamento, corte e encapsulamento/montagem do componente; e (v) serviço ao cliente.

2.2.2 Hardware Trojan: Definições Conceituais

O HT representa qualquer alteração maliciosa e deliberada no CI [41]. É uma modificação maliciosa, intencional e indesejada no CI, resultando em um comportamento incorreto de um dispositivo eletrônico quando em operação [31]. São modificações no circuito original inseridas por adversários com o objetivo de expor o hardware ou acessar dados ou software rodando nos sistemas que utilizam o *chip* [42]. As consequências de um circuito infectado podem envolver desde modificações na funcionalidade ou na especificação do hardware [31] [43], passando pelo vazamento de informações sensíveis [31] [20] [44] [45] [46] [27] ou mesmo ataques de negação de serviço (Denial of Service – DoS) [44] [31] [47] [42]. O hardware Trojan pode ser capaz de derrotar qualquer mecanismo de segurança, seja baseado em software ou hardware, subvertendo ou alterando a operação normal de um dispositivo infectado [31]. Tais inclusões maliciosas de fato agem como "espiões ou terroristas" no CI [21]. O que pode ser feito em milhões de linhas de código (programação de software), em tese, também pode ser feito com milhões de circuitos impressos em CIs [48].

2.2.3 Taxonomia do hardware Trojan

Diversas pesquisas vêm propondo classificações para o fenômeno hardware Trojan, descrevendo vários atributos associados, com o objetivo não só de estabelecer um estudo sistemático sobre o tema, mas de permitir o desenvolvimento de técnicas de detecção e mitigação para determinadas classes de HT [31].

Um estudo detalhado foi desenvolvido por Wang, Tehranipoor e Plusquellic [49] e baseia-se em três categorias principais: características físicas; características de ativação; e características de ação (Figura 2.11, adaptada de Wang, Tehranipoor e Plusquellic [49] e Tehranipoor e Koushanfar [42]). Os Trojans podem ser híbridos nessa classificação, ou seja, podem possuir mais de uma característica.

A classificação envolvendo características físicas diz respeito às diversas dimensões físicas possíveis de serem trabalhadas em uma implementação do Trojan, classificando-se em tipo, tamanho, estrutura e distribuição.

Do ponto de vista do "tipo", a implementação física classifica-se em funcional (envolve a adição ou subtração de transistores ou portas lógicas) e paramétrica (envolve a modificação de conexões metálicas já existentes ou mesmo na lógica do circuito) [49] [42].

O "tamanho"relaciona-se com a quantidade de componentes do chip que foram adicionados, deletados ou comprometidos [49] [42]. O tamanho pode ser um fator importante durante a ativação do HT, uma vez que Trojans mais compactos e com menos entradas tem probabilidade maior de serem ativados [49].

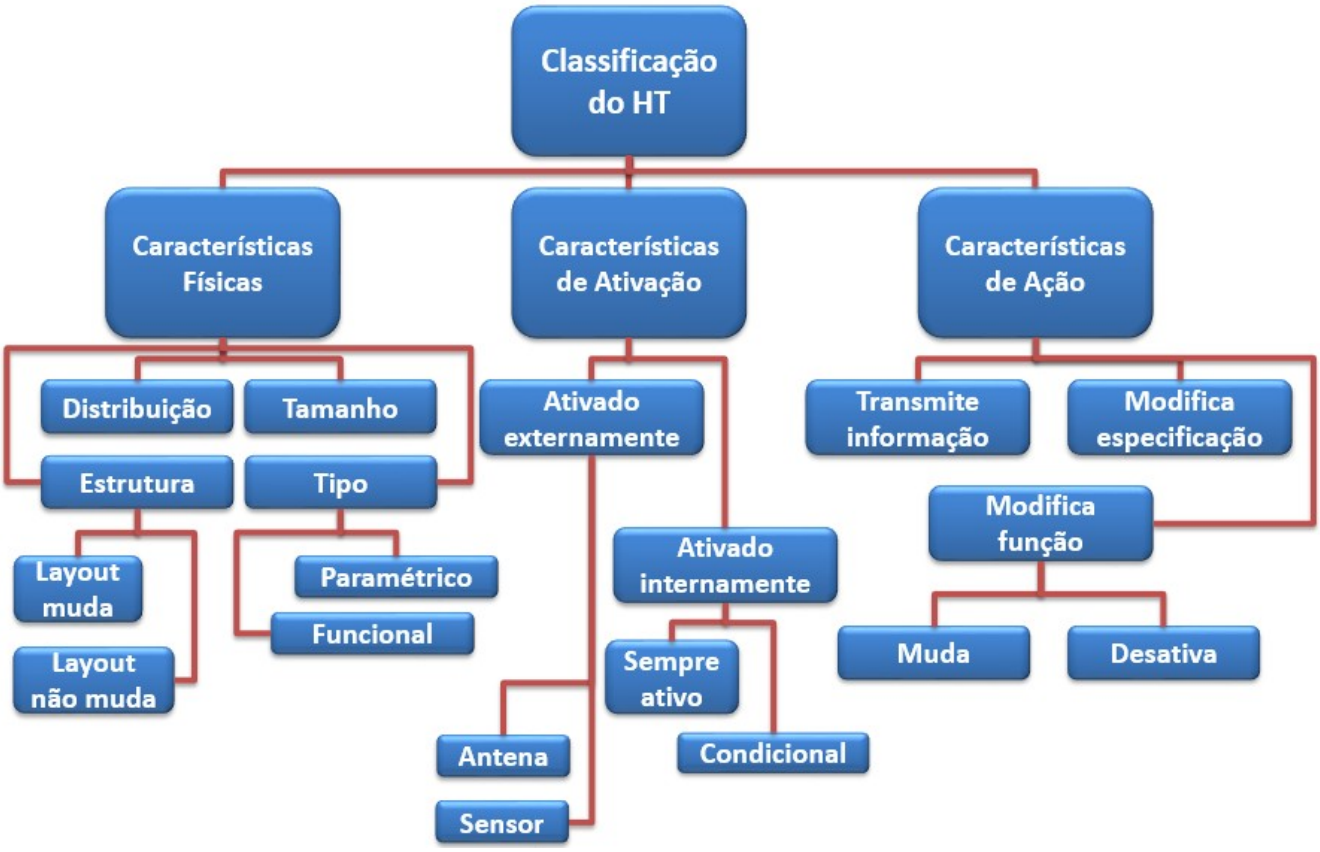

Figura 2.11: Taxonomia proposta para o HT, mostrando a classificação inicial em três categorias.

A "distribuição"relaciona-se com a localização do Trojan no layout físico do chip [49] [42]. Um HT pode ser implementado de forma concentrada em determinado ponto do chip, ou pode encontrar-se espalhado pelo layout do circuito [49].

Do ponto de vista da "estrutura", a implementação física pode ocorrer com ou sem a mudança do layout do circuito. Se o atacante é forçado a recriar o layout do chip para inserir o HT, então as dimensões do CI se alteram [49]. Qualquer mudança no layout físico pode modificar características de atraso (*delay*) e potência do chip, tornando mais fácil a detecção do Trojan [49] [42].

A classificação por meio de características de ativação enfoca a forma como o Trojan é ativado. O adversário que insere o código malicioso tornará difícil para o usuário a ativação do Trojan, como forma de prevenir uma ativação acidental e eventual detecção precoce na fase de testes. Assim, de uma perspectiva estatística, a ativação de um HT pode ser considerado um evento raro [49].

A ativação do HT pode ser externa, quando há a comunicação do Trojan com o mundo exterior ao chip, por meio da instalação de uma antena ou sensor no CI; e interna, quando

a ativação ocorre dentro do próprio CI [49]. Essa última ainda pode ser classificada como "sempre ativo" (quando o Trojan está permanentemente ativo e pode, a qualquer tempo, executar suas ações disruptivas); ou "baseado em condição", quando o Trojan permanece inativo, aguardando determinada condição ocorrer para ativá-lo [49].

E, por fim, a classificação por meio de características de ação tem enfoque no tipo de comportamento do HT. Ele pode modificar funções do chip; modificar especificações; ou transmitir informações [49] [42].

Outra taxonomia foi proposta por Chakraborty, Narasimhan e Bhunia [47]. Os autores, estendendo o estudo em Wolff *et al.* [50], propuseram uma classificação baseada no mecanismo de ativação (*trigger*) e na carga (*payload*) do HT (Figura 2.12, adaptada de Chakraborty, Narasimhan e Bhunia [47]).

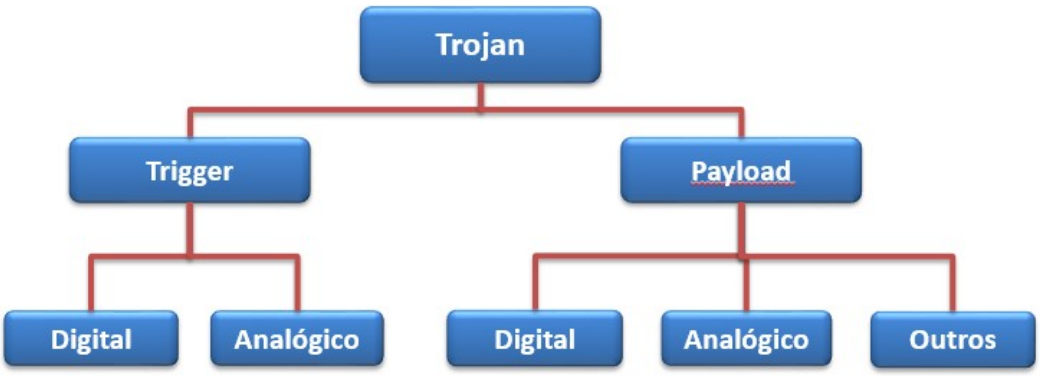

Figura 2.12: Taxonomia proposta para o HT, baseada no mecanismo de ativação e na carga do HT.

O mecanismo de ativação diz respeito à forma como o HT será ativado, produzindo seus efeitos indesejados [51]. Trojans ativados digitalmente se utilizam de condições bem específicas, uma sequência ou combinação binária, por exemplo, geralmente raras o bastante para não serem ativadas durante testes convencionais [49] [47]. Quando ativados de forma analógica, podem se utilizar de mecanismos implementados fisicamente no circuito, como sensores de temperatura que provocam a ativação a partir de determinada medição [41] [47] [52] [53] [54] [55] [49] [56] [27].

Do ponto de vista da carga (*payload*) do HT, aqui entendida como a parte do circuito ou a funcionalidade afetada [47] [21], tem-se também a classificação analógica ou digital. Trojans digitais podem, por exemplo, afetar os valores lógicos de determinados pontos do circuito, ou modificar o conteúdo em determinadas localizações da memória [47]. *Payloads* analógicos podem afetar parâmetros do circuito, tais como sua performance [57] [58].

Outras formas de *payload* podem ainda envolver ataques de negação de serviço [44] [31] [47] [42], nos quais há uma indisponibilidade do sistema causada pela ação do Trojan; e o vazamento de informações [31] [20] [44] [45] [46] [27].

Outra classificação foi proposta por Rajendran *et al* [41] com base em cinco atributos (Figura 2.13, adaptada de Rajendran *et al* [41]): 1) a fase do processo de criação do CI que é afetada; 2) o nível de abstração do hardware afetado; 3) a forma como o Trojan é ativado; 4) os efeitos gerais; e 5) a localização física do HT.

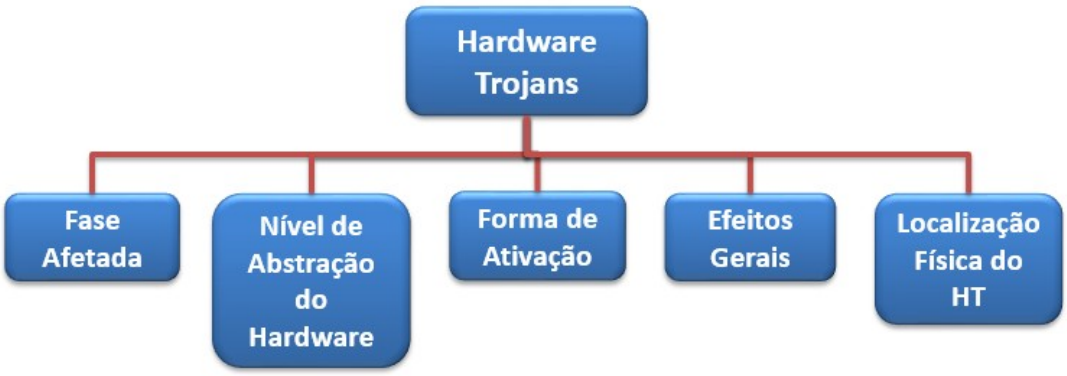

Figura 2.13: Taxonomia proposta para o HT com base em cinco atributos.

Quanto à fase afetada, os autores discutem possibilidades de inserção nas fases de especificação; design; fabricação; testes; e de montagem e empacotamento [41].

Quanto ao nível de abstração do hardware, a inserção pode ocorrer no nível do sistema; no ambiente de desenvolvimento; no nível do RT (RTL, *Register Transfer Level*, ou nível de transferência dos registros); no nível das portas lógicas; no nível dos transistores; e no nível físico [41].

Do ponto de vista da ativação, Rajendran *et al* [41] afirmam que alguns HTs são criados para permanecer sempre ativos, enquanto outros se mantém inertes até serem ativados por determinada condição ("gatilho"ou *trigger*). Uma vez ativados, podem permanecer nessa condição por tempo indeterminado ou retornar para a condição inerte após algum tempo.

O "gatilho"pode ser interno, quando o Trojan é ativado por um evento que ocorre dentro do chip, como um contador, por exemplo; ou externo, quando o HT é ativado por meio de uma entrada externa, como um interruptor ou mesmo um teclado [41].

Quanto aos efeitos gerais, os autores [41] os classificam em ações que: modificam funções; modificam especificações; vazam informação sensível; e negam serviços (DoS, *Denial of Service* ou negação de serviço).

Por fim, quanto à localização física, os pesquisadores discorrem sobre a possibilidade de inserção em componentes unitários ou de forma espalhada em múltiplos componentes,

agindo de forma independente ou em conjunto. Os Trojans podem ser localizados em unidades de processamento, na memória, em pontos de I/O (entrada/saída) ou na grade de energia.

2.2.4 Pontos de inserção do hardware Trojan

Dentre as fases envolvidas em um típico esquema de fabricação de circuitos integrados, as mais suscetíveis à inserção do HT são o design e a manufatura [47]. As possíveis ações maliciosas nessas fases são descritas a seguir [21]: no design, um agente não confiável que esteja envolvido no processo de escrita do IP (Intellectual Property ou Propriedade Intelectual, que constitui o desenho lógico de partes ou blocos funcionais do circuito integrado) pode alterar maliciosamente a lógica, inserindo o HT; ainda nesta fase, o uso de softwares do tipo EDA (Electronic Design Automation, ferramentas que facilitam o trabalho de design) corrompidos também pode resultar na inserção do código malicioso; e, finalmente, na fase de manufatura, é possível comprometer o CI a partir da ação de um agente mal intencionado utilizando técnicas de engenharia reversa.

Os pontos de ameaça com base em um modelo típico do mercado de CIs, composto essencialmente de cinco atores, são descritos abaixo [27]:

Fornecedores de Ferramentas EDA: Vendem as ferramentas EDA (Electronic Design Automation) aos fornecedores de IP e aos projetistas SoC. Tais ferramentas facilitam o trabalho de desenho e projeto de circuitos integrados.

Fornecedores de IP: São empresas especializadas na criação de IPs (Intellectual Property ou Propriedade Intelectual, que constitui o desenho lógico de partes ou blocos funcionais do CI).

Projetistas SoC: Criam e projetam produtos comerciais (SoC ou System on a Chip, CIs que contém todos os circuitos eletrônicos necessários para determinado sistema) que utilizam diversos IPs.

Fábricas: São empresas que manufaturam os CIs.

Usuários Finais: Empresas ou indivíduos que compram os produtos comerciais entregues pelos projetistas SoC.

As relações entre os atores são mostradas na Figura 2.14, adaptada de Li e Liu [27]. As setas representam o fluxo do serviço, do fornecedor ao cliente.

De acordo com o estudo [27], o HT pode ser implementado em diferentes fases do ciclo de vida do CI: ferramentas EDA, que são softwares, podem conter códigos maliciosos implementados por seus fornecedores de forma a alterar a lógica de criação dos CIs,

Figura 2.14: Modelo típico do mercado de circuitos integrados.

inserindo um HT no projeto, mesmo sem o conhecimento da equipe que opera a ferramenta; por outro lado, fornecedores de IP, agindo de forma maliciosa, podem inserir HTs em seus produtos, comprometendo toda a cadeia a partir dos projetistas SoC; estes, por sua vez, tem controle amplo sobre o projeto, podendo deliberadamente inserir alterações maliciosas na lógica dos circuitos, antes de serem manufaturados nas fábricas de CI; e, finalmente, nas próprias fábricas também é possível a inserção de HTs por agentes maliciosos que tenham acesso às etapas de fabricação. É o exemplo do uso de dopantes com a finalidade de alterar as propriedades elétricas do CI, como será visto na próxima sessão.

2.2.5 Implementações de hardware Trojan

Compreendendo que a ameaça existe e é explorada em diversos momentos na fabricação do circuito integrado, é importante entender como ela é criada e se há meios de detectá-la. De fato, há vários estudos abordando o tema. Conforme Becker *et al* [20], os esforços de pesquisa concentram-se basicamente em duas áreas: uma relativa ao design e implementação do HT; e outra lidando com o desafio de detectar a ameaça.

A seguir, serão apresentados casos de implementação do HT. A seção seguinte tratará em detalhes as possibilidades de detecção.

King *et al.* [28] apresentaram uma forma combinada de ataque envolvendo hardware e software. Neste ataque, um hardware Trojan implementado no CI dá suporte para um ataque por meio do software, ao permitir que o agente malicioso tenha acesso privilegiado

(*root* [6]) ao sistema operacional [23]. Tal implementação permite ataques poderosos e de propósito geral, embora utilize pequena quantidade de hardware adicional no circuito [28].

Shiyanovskii *et al.* [59] apresentaram um HT que implementa um ataque de negação de serviço (DoS) ao degradar a performance do chip de forma gradual. As modificações podem manter os parâmetros iniciais de performance dentro dos padrões aceitáveis de variação, dessa forma permanecendo indetectável pelos testes tradicionais.

A viabilidade de inserção de hardware malicioso em circuitos mapeados em FPGAs[7] foi discutida por Chakraborty *et al.* [60]. Em particular, os pesquisadores se utilizaram de um HT baseado em um anel-oscilador [8] capaz de reduzir o tempo de vida do chip através do aumento da temperatura de operação do circuito.

Em Subramani *et al.* [61], estudou-se a possibilidade de um ataque de HT em redes *wireless* a partir da infecção de um transmissor 802.11a/g, permitindo ao agente malicioso o vazamento de informações sensíveis na conexão.

Conforme abordado no Capítulo 1, o presente trabalho não objetiva exaurir as várias formas de implementação do HT. No entanto, como forma de ilustrar os conceitos e demonstrar potencialidades e complexidades da ameaça, discutiremos em detalhes o chamado "Stealthy Dopant-Level Hardware Trojan" (hardware Trojan furtivo implementado no nível do dopante), proposto por Becker *et al* [20].

Trata-se de um HT com duas características peculiares: ele é furtivo ou dissimulado, o que significa que sua detecção não é possível pelos meios convencionais; e ele é implementado no nível do "dopante", ou seja, utiliza-se do processo de dopagem do semicondutor. Conforme Pikma [62], o processo de dopagem envolve a adição de impurezas no material semicondutor, modificando suas propriedades elétricas.

Por exemplo, a adição de átomos de Fósforo ao silício puro atribui-lhe polaridade negativa, enquanto que a adição de átomos de Boro cria polaridade positiva. Esse processo de dopagem é um recurso comumente utilizado na fabricação de transistores que compõem o circuito integrado. A questão aqui é que o agente malicioso se utiliza desse mesmo procedimento para a implementação do HT, ou seja, ao manipular as polaridades dos transistores presentes no circuito integrado, é possível criar uma lógica maliciosa no funcionamento do CI.

Utilizando-se dessa técnica, Becker *et al* [20] provaram que é possível reduzir a segurança dos números aleatórios gerados pelo Random Number Generator - RNG (Gerador de Números Randômicos) dos processadores Ivy Bridge da Intel (linha de processadores

[6] Operador com todas as permissões administrativas de sistemas Unix e outros [23].

[7] Field-Programmable Gate Array, ou Matriz de Portas Programáveis em Campo, é uma espécie de CI projetado para ser programado após a manufatura. Dessa forma, ele possui blocos lógicos reprogramáveis passíveis de configuração em campo, ou seja, pelo consumidor ou projetista após a fabricação [23].

[8] Um anel-oscilador é um circuito serial com número ímpar de portas lógicas e com retorno na entrada. A frequência resultante é uma função do número de portas, da temperatura, dentre outros [23].

de 22 nanômetros da marca americana), a partir da implementação de códigos maliciosos por meio de dopantes. O RNG do chip Intel é uma implementação embarcada no hardware que produz números randômicos de 128 bits a partir de ruídos termais.

Com a ação do hardware Trojan, foi possível reduzir a complexidade da saída do RNG de 128 bits para "n" bits, no qual "n" pode ser definido pelo atacante, a depender do número de transistores modificados. Essa possibilidade constitui uma importante quebra de segurança na funcionalidade do CI.

Observa-se, ainda, que a ação é possível a partir de modificações em poucos transistores. Em uma das implementações, os autores modificaram apenas 896 transistores (dentre os milhões existentes no chip).

Tal tipo de implementação, como mencionado, é extremamente difícil de ser detectada. Conforme se concluiu no estudo conduzido por Pikma [62], uma vez que o leiaute e a fiação do circuito permanecem exatamente os mesmos quando comparados a um CI não infectado, e considerando que a única diferença está no nível atômico do substrato do semicondutor, esse tipo de HT escapa às formas tradicionais de detecção, como a inspeção ótica, os testes funcionais, ou mesmo a inspeção por uso de *golden chips* (CIs não infectados usados como modelos para comparações).

2.2.6 Detecção de hardware Trojan

Conforme visto, a inserção do HT é possível em diversas fases da criação do CI. Segundo Abramovici e Bradley [63], não há métodos confiáveis que garantam a detecção de HT antes da utilização efetiva do *chip*. Não há uma solução mágica para detectar todos os tipos de HT [31]. Assumindo que o atacante pode maliciosamente alterar o design antes e após a manufatura, tem-se que a detecção de tais alterações é extremamente difícil, por diversas razões [42].

Primeiro, dada a quantidade e a complexidade dos IP *cores* utilizados nos SoCs, detectar pequenas modificações no CI é extremamente difícil [42].

Segundo, as características nanométricas dos CIs fazem com que detecções por meio de inspeção física ou engenharia reversa (destrutiva) sejam muito difíceis e caras. Ainda, a engenharia reversa destrutiva (feita em uma amostra) não garante que os demais CIs estejam livres do HT, em especial quando os Trojans são inseridos seletivamente em determinada porção da população de *chips* [42].

Terceiro, circuitos de HT são geralmente ativados sob condições muito específicas [49] (por exemplo, detectando um sinal específico, como temperatura ou potência), o que os fazem improváveis de serem ativados ou detectados por meio de estímulos funcionais ou randômicos [42].

Quarto, testes utilizados para detectar falhas de manufatura, como falhas de atraso (*delay*) não garantem a detecção dos Trojans. Tais testes operam no nível do *netlist* (descrição da conectividade de um circuito eletrônico [23]) de circuitos livres do Trojan e, consequentemente, não são capazes de ativar ou detectar os HTs [42].

Finalmente, uma vez que o tamanho das características físicas de CIs vem reduzindo em virtude de aprimoramentos na técnica de litografia (processo que imrime a imagem do circuito), variações no processo e no ambiente tem um impacto cada vez maior na integridade da parametria dos circuitos. Assim, a detecção de HT utilizando simples análise desses sinais paramétricos seria inefetiva [42].

De fato, há variadas técnicas para a detecção do HT, mas são apenas capazes de detectar classes específicas de Trojan [31]. É de se esperar, como ocorre com os *malwares* de software, que os agentes que projetam HT tentarão escapar de técnicas já conhecidas de detecção, de forma a ter sucesso em seus objetivos [31].

Uma visão apresentada por pesquisadores [47] classifica as formas de detecção em destrutivas e não destrutivas (Figura 2.15, adaptada de Chakraborty [47]).

Figura 2.15: Tipos de técnicas de detecção de Hardware Trojans.

Técnicas destrutivas destroem completamente o CI examinado, o que prejudica a utilidade dessas técnicas [31]. A amostra de CI analisada é submetida à de-metalização usando polimento mecânico químico (Chemical Mechanical Polishing, ou CMP, processo

utilizado na engenharia reversa no qual o CI sofre ações químicas e mecânicas) seguido pelo escaneamento SEM (Scanning Electron Microscope, microscópio que produz imagens de uma amostra escaneando a superfície com um feixe de elétrons) [47]. No entanto, tal abordagem é extremamente cara e leva bastante tempo para ser feita [64] [47], além de possuir baixa escalabilidade com o aumento da complexidade dos componentes de um chip [47]. Além disso, o resultado da analise da amostra não pode ser estendido para o restante do lote manufaturado, uma vez que o adversário pode ter comprometido apenas uma pequena parcela da população de CI manufaturados [47]. Assim, é engenharia reversa destrutiva não é uma técnica eficiente [63].

Por outro lado, as técnicas não destrutivas preservam o *chip*, e são divididas em dois tipos [55] [47]: invasivas, que modificam o design do chip com o objetivo de embarcar funcionalidades capazes de detectar o Trojan; e não invasivas, que preservam o design original do circuito.

As técnicas invasivas, por sua vez, podem atuar prevenindo a inserção de Trojans durante o design ou a manufatura; ou atuar de forma assistiva, no circuito já infectado [47].

As técnicas não invasivas também se apresentam em dois tipos: as que atuam em tempo de execução do chip, ou seja, procuram monitorar o comportamento do chip quando em atuação; e as que atuam em tempo de teste, ou seja, procuram detectar HT antes que os CI sejam empregados em algum sistema ou equipamento [47].

Outros pesquisadores [42] categorizam os métodos de detecção em "Side-Channel Analysis"(análise de canal lateral) e "Ativação do Trojan", que são, em essência, soluções no nível do chip e no nível da arquitetura.

Sinais de canal lateral são parâmetros físicos ou lógicos modificados de forma não intencional como subproduto de outra tarefa [23]. Por exemplo, determinado processamento no *chip* pode provocar alterações no calor gerado ou no consumo de energia [31].

De acordo com os autores [42], sinais de canal lateral, incluindo tempo e potência, podem ser usados para a detecção de Trojans. Isso porque HT tipicamente alteram características paramétricas do design, por exemplo degradando a performance, mudando as características de potência do chip, ou mesmo introduzindo problemas de confiabilidade.

Isso acaba por influenciar características de potência ou atraso nas conexões ou portas lógicas do circuito infectado [42], que podem ser analisadas por equipamentos sensíveis, levantando a suspeita da presença do Trojan.

Sinais de canais laterais baseados em consumo de energia oferecem visibilidade da estrutura interna e das atividades internas do CI, permitindo a detecção de HT sem necessariamente ativá-los [42].

Já os sinais de canais laterais baseados em tempo podem detectar a presença do HT se o circuito é testado usando testes de *delay* eficientes, sensíveis a pequenas modificações

no *delay* do circuito ao longo de caminhos afetados e que podem efetivamente diferenciar o que é um HT do que seriam possíveis variações (normais) do processo.

A outra categorização apresentada pelos autores baseia-se no tipo de ativação do Trojan. Estratégias de ativação do HT podem acelerar o processo de detecção deles, e em alguns casos tem sido combinadas com análise de potência durante a implementação [42]. Se uma determinada parte do circuito Trojan é ativada, o circuito consumirá maior energia, ajudando a diferenciar os traços energéticos de circuitos livres de Trojans em comparação a circuitos infectados [42].

2.3 O hardware Trojan e suas implicações no contexto da segurança da informação e da segurança cibernética

A ameaça do HT já foi cogitada há décadas. Em 1994, Schwartau [65], em sua obra "Information Warfare"(Guerra de Informação), já afirmava que os CIs nem sempre são o que aparentam ser. Para o pesquisador, a possibilidade de falhas intencionais em CIs poderia ser explorada por agentes maliciosos, a exemplo do que já ocorria com as implementações em software.

Embora a possibilidade de uso malicioso de circuitos integrados não seja uma novidade, as preocupações com o fenômeno hardware Trojan são relativamente recentes e se tornaram mais incisivas na última década [31].

Em 2005, o Departamento de Defesa dos Estados Unidos publicou um estudo [66] sobre a segurança no processo de fabricação de circuitos de alta performance. O documento alertava para os riscos envolvidos na migração do processo de fabricação de CIs dos Estados Unidos para outros países, em particular nos *chips* utilizados em sistemas de defesa nacional, nas infraestruturas críticas e nas aplicações ligadas às áreas de inteligência.

De fato, a preocupação com a confiança dos CIs vem crescendo com a globalização de sua cadeia de suprimentos [42] [20] [67] [68]. Há algumas décadas, era comum que uma mesma fábrica acumulasse todas as funções do processo de fabricação, do projeto à manufatura. Por razões econômicas, o modelo tornou-se inviável e a separação entre o design e a manufatura tornou-se inevitável [26]. Por um lado, os designers passaram a focar em sua competência principal, sem arcar com os altos custos de se manter uma planta de construção; por outro, as indústrias de manufatura puderam viabilizar os elevados custos de suas instalações altamente intensivas em tecnologia, buscando a plena produção ao atender diversos clientes da área de design [26].

E, não raro, as indústrias de manufatura estão espalhadas fora dos territórios nacionais [45], principalmente em países asiáticos [31] [26]. Isso provoca, naturalmente, uma perda de controle na cadeia de suprimentos.

Soma-se a isso o aumento da complexidade dos próprios CIs. Desde a década de 60, o número de transistores (componente básico do CI utilizado na implementação das funções lógicas) embarcados nos circuitos eletrônicos vem dobrando a cada dois anos, evoluindo de algumas centenas para os atuais bilhões de transistores comumente implementados em um único CI [26].

Assim, detectar um código malicioso em meio a tamanha complexidade tornou-se um grande desafio. E, de fato, atacantes cibernéticos sempre procuram conduzir seus ataques de forma tão furtiva quanto possível, o que os leva a implementar seus ataques, tanto quanto possível, nos mais baixos níveis de abstração, como o hardware [23].

Vale lembrar que produtos com características mais complexas podem exigir CIs específicos, os quais poucos fabricantes irão fornecer, elevando a dependência de outros fornecedores para o produto final.

2.3.1 Caso Síria

Em 6 de setembro de 2007, aviões israelenses F-15 Eagle e F-16 Falcon entraram no espaço aéreo Sírio, vindos da Turquia, e bombardearam o que seriam instalações nucleares projetadas pela Coreia do Norte. A imprensa chegou a divulgar ainda suposto envolvimento dos EUA no ataque [48].

Não obstante as complexas implicações políticas do episódio, o que chamou a atenção foi o fato de que o sistema de defesa antiaérea da Síria permaneceu inoperante na ocasião, o que permitiu que os aviões de ataque entrassem e saíssem sem ser alvejados. A Síria havia investido milhões de dólares nos sistemas de defesa antiaérea comprados da Rússia.

Pesquisadores vem trabalhando a hipótese de que o sistema antiaéreo sírio estaria infectado com alguma espécie de *backdoor*[9] inserido nos chips do sistema [51]. Cogita-se ainda a hipótese de ter sido, de fato, um hardware Trojan implementado nos sistemas sírios [27]. Em outro artigo, Moein *et al.* [69] destacam a possibilidade de microprocessadores comerciais *off-the-shelf* [10] terem sido adquiridos com um *backdoor* utilizado para desativá-los no momento oportuno. Ou seja, a falha teria sido intencionalmente ativada por meio de um gatilho (*trigger*) [22], em momento definido pelo atacante.

[9] O backdoor é uma espécie de malware que, após incluído em um sistema, é usado para assegurar o acesso futuro ao computador comprometido, permitindo que ele seja acessado remotamente, sem que haja necessidade de recorrer novamente aos métodos utilizados na realização da invasão ou infecção e, na maioria dos casos, sem que seja notado [4].

[10] Componentes eletrônicos prontos, de prateleira, com acesso direto para aquisições [23]

O caso Síria, embora ainda envolto em grande mistério, dado que abrange intricadas questões geopolíticas, é um caso que certamente traz reflexões, no contexto da SIC e da SegCiber, sobre o potencial lesivo do uso de implementações maliciosas no hardware, ainda que em conjunto com outras práticas tradicionais de guerra.

2.4 Planejamento Estratégico, Tático e Operacional

2.4.1 Planejamento Estratégico

O campo de estudos sobre planejamento estratégico envolve um extenso histórico que inclui o surgimento de múltiplas teorias e enfoques, eventualmente competindo entre si. Duas escolas de pensamento receberam destaque ao longo do tempo: a escola do planejamento ou racional, e a escola de aprendizagem ou adaptativa, que representam maneiras opostas de abordar o tema [70]. Para a escola racional, o planejamento é um processo estruturado e controlado, enquanto que a escola adaptativa vê o processo de planejamento como algo que não pode ser deliberadamente controlado, uma vez que ele deve ser adaptado e atualizado ao longo do tempo [71] [72].

Na prática atual, parece não haver uma demarcação clara entre as duas escolas, e o debate passou a considerar uma abordagem mais integradora das teorias [73].

Do ponto de vista conceitual, o planejamento estratégico envolve um esforço disciplinado com o objetivo de produzir decisões e ações que formarão e guiarão as atividades e os propósitos organizacionais [74]. Segundo Maximiniano [75], o planejamento estratégico é o processo de estruturar e esclarecer os caminhos da organização e os objetivos que ela deve alcançar. É um processo organizacional compreensivo de adaptações através da aprovação, da tomada de decisão e da avaliação [76]. Trata-se de uma metodologia gerencial que permite estabelecer a direção a ser seguida pela organização, visando maior grau de interação com o ambiente [77].

Para Almeida [78], é uma ferramenta administrativa que busca um ordenamento das ideias do planejador, visando identificar o caminho que deve ser seguido pela organização. Após o ordenamento das ideias, deve haver um ordenamento das ações, ou seja, a implementação do plano estratégico para que a empresa alcance seus objetivos sem desperdício de recursos.

O planejamento estratégico é o primeiro item a ser abordado pela administração estratégica, pois possibilita o planejamento do desenvolvimento e de mudanças organizacionais [79]. Através do planejamento estratégico, os recursos podem ser concentrados em um número limitado de objetivos, dessa forma auxiliando a organização a manter o foco,

garantindo que seus membros irão trabalhar na mesma direção, além de eventualmente avaliar e ajustar essa direção em resposta a um ambiente sempre em mudança [74].

Para Chiavenato [80], o planejamento estratégico apresenta cinco características fundamentais: (i) ele está relacionado com a adaptação da organização a um ambiente mutável, portanto sujeito às incertezas a respeito dos eventos ambientais; (ii) é orientado para o futuro, ou seja, seu horizonte de tempo geralmente é o longo prazo; (iii) é compreensivo, o que significa que ele envolve a organização como um todo, abarcando todos os seus recursos, no sentido de obter efeitos sinérgicos com todas as capacidades e potencialidades da organização; (iv) é um processo de construção de consenso, dada a diversidade de interesses e necessidades das partes envolvidas; e (v) o planejamento estratégico é uma forma de aprendizagem organizacional, uma vez que está orientado para a adaptação da organização ao contexto ambiental e representa uma constante tentativa de ajustar-se a um ambiente complexo, competitivo e mutável.

O planejamento estratégico se assenta ainda sobre três pilares: a visão de futuro; os fatores ambientais externos; e os fatores organizacionais internos [76].

A partir da visão de futuro, constrói-se o consenso sobre o futuro que se almeja (mundo em um estado ideal). Mas, para que esse estado seja alcançado, é necessário entender os fatores organizacionais (internos) e as influências ambientais (externas) [76], para que, a partir de então, os objetivos estratégicos sejam traçados.

Há uma variedade de perspectivas, modelos e abordagens utilizadas no planejamento estratégico. A forma como o plano estratégico é desenvolvido depende da natureza da liderança da organização, da cultura organizacional, da complexidade da organização e de seu ambiente, e do tamanho da organização [74].

Para Maximiano [75], um processo sistemático de planejamento estratégico compreende os seguintes componentes principais:

1. Análise da situação estratégica presente (onde estamos?);
2. Análise do ambiente (quais são as ameaças e oportunidades do ambiente?);
3. Análise interna (quais são os pontos fortes e fracos dos sistemas internos da organização?);
4. Elaboração do plano estratégico (para onde devemos ir? O que devemos fazer para chegar lá?).

Outra abordagem semelhante pode ser observada em Certo [81]. Segundo o autor, o processo de estratégia é dividido em cinco etapas principais:

- Execução de análise do ambiente, na qual são identificados riscos e oportunidades que tem influência na realização das metas organizacionais;

- Estabelecimento de diretriz organizacional, que aborda, em essência, o estabelecimento da missão e dos objetivos organizacionais;
- Formulação de estratégia organizacional, que visa o estabelecimento de ações apropriadas ao alcance dos objetivos;
- Implementação da estratégia organizacional, que compreende a colocação da estratégia em ação;
- Exercício de controle estratégico, que envolve atividades que objetivam o desenvolvimento daquilo que foi planejado, englobando a comparação do desempenho organizacional real com as metas e padrões estabelecidos.

2.4.2 Planejamento Tático e Operacional

Enquanto podemos definir estratégia como a mobilização de recursos no âmbito global visando atingir os objetivos no longo prazo, a tática é um esquema específico de emprego de recursos dentro de uma estratégia geral [80].

Assim, a diferença básica entre estratégia e tática reside em três aspectos: (i) a estratégia engloba a organização como um todo, pois procura alcançar objetivos organizacionais globais, enquanto que a tática se refere a um dos componentes da organização (unidades), pois objetiva alcançar objetivos específicos; (ii) a estratégia se refere aos objetivos situados no longo prazo, enquanto a tática se refere a objetivos de médio prazo; (iii) para a implementação da estratégia, são necessárias muitas táticas que se sucedem ordenadamente no tempo [80].

No ambiente organizacional, o que determina as principais intenções da empresa, o seu curso e o tempo para a concretização da estratégia, são as metas e os objetivos [79]. Metas são pontos ou posições a serem atingidas no futuro, sendo um conceito utilizado no Balanced Scorecard, conhecida metodologia de planejamento e gestão estratégica, que será analisada em tópico a seguir.

O planejamento estratégico é desdobrado em vários planejamentos táticos, enquanto esses se desdobram em planos operacionais para sua realização [76] [82].

Segundo Maximiano [75], o planejamento operacional é o processo de definir atividades e recursos, e compreende as seguintes etapas ou decisões principais:

- Análise dos objetivos, no qual o objetivo principal é dividido em objetivos menores, formando uma cadeia de meios e fins;
- Planejamento do uso do tempo, em que as atividades necessárias para atingir os objetivos são identificadas e tem seus tempos de duração estimados;

- Planejamento dos recursos, ou seja, após a identificação das atividades, realiza-se a definição de recursos materiais e humanos necessários para realizá-las, bem como os custos envolvidos.
- Avaliação dos riscos, de forma a possibilitar o planejamento de ações que reduzam a ocorrência desses riscos;
- Previsão dos meios de controle das atividades, do consumo de recursos, dos riscos, dos objetivos e de outras variáveis que tenham sido incluídas nos planos.

No nível operacional, portanto, são definidas formas de desenvolvimento e de implementação de resultados específicos a serem alcançados [81].

2.4.3 Balanced Scorecard

O Balanced Scorecard (BSC) nasceu de um estudo conduzido em 1990 por Robert Kaplan, um professor de Harvard, e pelo consultor David Norton. Os pesquisadores conduziam um estudo junto com empresas locais que procurava explorar novos métodos de mediar a performance organizacional, pois acreditavam que as medidas financeiras de performance utilizadas até então eram inefetivas para o atingimento dos objetivos organizacionais [83]. A ideia do grupo era discutir alternativas que capturassem outras atividades da organização, como questões ligadas aos clientes, processos internos de negócio, atividades de funcionários e preocupações de stakeholders.

Mais tarde, em 1992, Robert Kaplan e David Norton publicariam então os primeiros estudos da nova ferramenta, que objetiva o estabelecimento de um processo estruturado para a criação de medidas financeiras e não financeiras, representadas por objetivos estratégicos e metas em todos os níveis, possibilitando a integração entre esses grupos e proporcionando o alinhamento de toda a organização [79].

De acordo com o Balanced Scorecard Institute [84], o BSC é um sistema de planejamento e gestão estratégica que as organizações utilizam para: (i) comunicar os objetivos que desejam atingir; (ii) alinhar as atividades diárias realizadas pela organização com sua própria estratégia organizacional; (iii) priorizar projetos, produtos e serviços; e (iv) medir e monitorar o progresso na direção de objetivos estratégicos.

O valor dessa metodologia reside na capacidade de traduzir a visão e a estratégia em ações que de fato contribuam para o alcance dos objetivos estratégicos, além de prover um sistema de retroalimentação que permite o ajuste e o aprimoramento contínuo por meio do acompanhamento de indicadores e metas [12].

O BSC controla desde a identificação das necessidades até a motivação das melhorias dos processos e produtos, criando um ambiente propício ao alinhamento estratégico organizacional [79].

Quatro conceitos são importantes para o entendimento da metodologia [84]: (i) objetivos estratégicos, que envolvem atividades contínuas de aprimoramento necessárias ao alcance do sucesso desejado; (ii) indicadores, que medem a performance organizacional; (iii) metas, que representam os níveis desejados de performance associados a cada indicador; e (iv) iniciativas estratégicas, que são projetos que ajudarão no alcance das metas.

Iniciativas envolvem as ações, processos, projetos e planos que farão as metas serem atingidas. Em determinado momento, certamente uma organização estará perseguindo uma série de diferentes iniciativas, mas é importante que se dê atenção àquelas que, de fato, estejam contribuindo para os objetivos estratégicos [83].

Na construção das iniciativas estratégicas, quatro passos são importantes [83]: primeiro, é necessário que um inventário de todas as iniciativas correntes seja levantado; após, as iniciativas devem ser mapeadas em relação aos objetivos já declarados no BSC; em seguida, iniciativas consideradas não estratégicas são descartadas; e, por fim, as iniciativas remanescentes são priorizadas.

Portanto, enquanto no nível estratégico o BSC declara os objetivos estratégicos da organização, no nível tático e operacional cria-se um sistema de indicadores, metas e iniciativas que possibilita um acompanhamento do alcance dos objetivos. Uma vez que ações e incrementos nos processos críticos não possibilitem ganhos financeiros a longo prazo, fica evidente que se trata de uma melhoria apenas tático-operacional, não estratégica [85].

O BSC mede o desempenho organizacional sob quatro perspectivas equilibradas (Figura 2.16, adaptada de Balanced Scorecard Institute [84]): financeira, do cliente, dos processos internos da organização, e do aprendizado e crescimento, constituindo-se, não em mera ferramenta de controle, mas em um sistema de comunicação e aprendizado [86].

Na visão de Costa [86], pode-se descrever resumidamente cada uma das quatro perspectivas como se segue: (i) financeira, que se traduz na crença de que a organização deve crescer e gerar riqueza aos seus acionistas; (ii) do cliente, na qual são identificados os segmentos de clientes e mercados nos quais se competirá, e as medidas de desempenho nesses segmentos-alvo, além das medidas específicas de criação de valor aos clientes; (iii) dos processos internos, na qual são identificados os processos internos críticos nos quais a organização deve ser excelente; e (iv) de aprendizado e crescimento, que identifica a infraestrutura que a organização deve manter para gerar crescimento e melhoria a longo prazo, cujas fontes principais de aprendizado e crescimento são pessoas, sistemas e procedimentos organizacionais.

O BSC deve então explicitar as relações entre os objetivos estratégicos e as medidas e vetores de desempenho em suas perspectivas, para que possam ser gerenciadas e validadas [86].

Tais relações são evidenciadas no Mapa Estratégico (Figura 2.17, adaptada de BSC

Figura 2.16: Perspectivas do Balanced Scorecard.

Institute [84]). Nele, a cadeia de causa e efeito entre objetivos (e indicadores) deve perpassar todas as perspectivas do BSC [85].

Inicialmente considerado domínio exclusivo das organizações privadas com fins lucrativos, o BSC passou a ser traduzido e efetivamente implementado em organizações sem fins lucrativos e no setor público. Tais organizações aprenderam que, por meio de pequenas modificações no *framework* do BSC, eram capazes de demonstrar às partes interessadas o valor que elas eram capazes de entregar, e os passos que estavam seguindo para a consecução de suas missões [83].

Felix, Felix e Timóteo [79] estudaram adequações do BSC para a gestão estratégica nas organizações públicas, em particular a Administração Pública Federal no Brasil.

Para os autores, embora os setores público e privado tenham como foco a preocupação em satisfazer seus "clientes", eles diferem quanto à amplitude de suas metas e ações, quanto ao perfil de seus clientes e na forma como utilizam os recursos financeiros.

Os autores propuseram então um modelo adaptado do BSC para as organizações públicas brasileiras, que chamaram de BSC.Gov. O modelo envolve cinco perspectivas que, como no BSC original, criam relações de causa e efeito (Figura 2.18, adaptada de

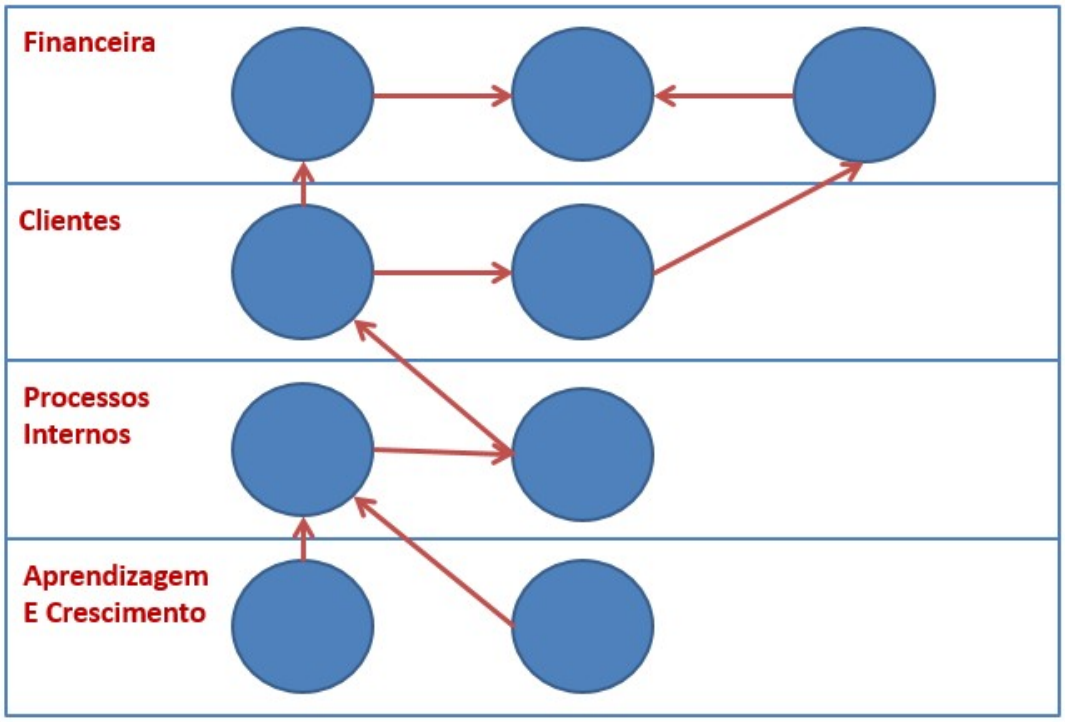

Figura 2.17: Mapa Estratégico hipotético do BSC, mostrando as relações de causa e efeito (setas) entre Objetivos Estratégicos (círculos).

Felix, Felix e Timóteo [79]):

De acordo com o estudo, as perspectivas propostas são assim entendidas, conforme exposto na Tabela 2.9:

As limitações encontradas após a comparação entre a aplicação do BSC no setor público e privado ocorreram, basicamente, em duas perspectivas: financeira e clientes [79]. A primeira, no setor privado, é voltada para a obtenção de lucro a acionistas e stakeholders, ao contrário do setor público, que articula recursos orçamentários limitados para a consecução de competências e políticas públicas previstas em lei. Na segunda, clientes, o setor privado busca o atendimento, muitas vezes de forma personalizada, das necessidades e desejos do mercado, maximizando as vendas e a entrega de valor. Para o setor público, que tem na sociedade seu cliente, o atendimento objetiva o alcance do interesse coletivo, despersonalizado e indisponível [11].

[11] Significa que sendo interesses qualificados como próprios da coletividade — internos ao setor público — não se encontram à livre disposição de quem quer que seja por inapropriáveis. O próprio órgão administrativo que os representa não tem disponibilidade sobre eles, no sentido de que lhe incumbe apenas curá-los — o que é também um dever — na estrita conformidade do que dispuser a lei [87]

Figura 2.18: Relações de causa e efeito das perspectivas do BSC.Gov.

2.4.4 Metodologia 5W2H

Conforme visto, o Balanced Scorecard prevê a criação de iniciativas estratégicas, que são projetos que ajudarão no alcance das metas [84]. Segundo Kaplan [88], tais iniciativas são ações que movem a organização na direção de seus objetivos estratégicos de longo prazo.

Walter [89] propõe, no contexto de aplicação do BSC, a utilização da metodologia 5W2H para a construção de um plano de ação.

O método 5W2H é uma ferramenta que permite a estruturação organizada do pensamento, materializando ideias antes da implementação propriamente dita [90].

O acrônimo 5W2H (Figura 2.19, extraído de Nakagawa [91]) vem das palavras em inglês What, When, Why, Where, Who, How e How Much (O que? Quando? Por que? Onde? Quem? Como? Quanto?), que são perguntas que procuram orientar as ações de forma a mantê-las alinhadas aos objetivos estratégicos que se pretende atingir [89].

Segundo Nakagawa [91], as sete perguntas compõem campos em que devem constar as seguintes informações:

- Ação ou atividade que deve ser executada ou o problema ou o desafio que deve ser solucionado (*what*);
- Cronograma sobre quando ocorrerão os procedimentos (*when*);

Tabela 2.9: Detalhamento das Perspectivas Propostas no BSC.Gov

Orçamentária	Para cumprirmos nossa missão, como devemos realizar nossos custos e investimentos e sermos vistos pelos órgãos de controle?
Aprendizado, Crescimento e Processos Internos	Para adquirir a capacidade de mudar e inovar, como devemos cuidar de nossos servidores públicos e colaboradores? Para aumentar a qualidade dos serviços à sociedade e reduzir os custos, como devemos promover a melhoria das comunicações e de nossos processos internos?
Relações Governamentais	Para melhor articular e viabilizar as ações intra e entre órgãos e instituições, como devemos promover as relações entre as demais perspectivas?
Administração Pública Federal	Para alcançar nossa visão, como devemos ser vistos pelos órgãos da administração direta e indireta?
Cidadão e Sociedade	Para alcançar a nossa visão, como devemos ser vistos pela sociedade?

5W					2H	
What	**Why**	**Who**	**Where**	**When**	**How**	**How much**
O que	Por que	Quem	Onde	Quando	Como	Quanto
Ação, problema, desafio	Justificativa, explicação, motivo	Responsável	Local	Prazo, cronograma	Procedimentos, etapas	Custo, desembolsos

Figura 2.19: Técnica 5W2H.

- Justificativa dos motivos e objetivos daquilo estar sendo executado ou solucionado (*why*);
- Informação sobre onde cada um dos procedimentos será executado (*where*);
- Definição de quem serão os responsáveis pela execução do que foi planejado (*who*);

- Explicação sobre como serão executados os procedimentos para atingir os objetivos pré-estabelecidos (*how*); e
- Limitação de quanto custará cada procedimento e o custo total do que será feito (*how much*).

O método 5W2H é utilizado principalmente na elaboração de planos de ação, através de definição de responsabilidades, métodos, prazos, objetivos e recursos associados [92].

Capítulo 3

Metodologia

3.1 Etapas metodológicas

Segundo Gil [93], o problema de pesquisa deve ser delimitado a uma dimensão viável. Estabelecem-se limites em relação ao assunto, à extensão, ao prazo, dentre outros [94]. A delimitação de escopo permite trabalhar de maneira focada, obtendo dados relevantes dentro do tempo delimitado para a execução da pesquisa [95].

Com a finalidade de cumprir os objetivos definidos na pesquisa, estruturou-se metodologia com base em etapas sequenciais de trabalho, definidas da seguinte forma: etapa I - Fundamentação; etapa II - Desenvolvimento; e etapa III - Proposições.

A Figura 3.1, de criação do autor, apresenta a Estrutura Analítica de Projeto, que representa uma visão sobre a subdivisão das entregas e do trabalho do projeto em componentes menores e mais facilmente gerenciáveis [96].

As etapas serão detalhadas a seguir.

3.1.1 Etapa I - Fundamentação

A primeira etapa, Fundamentação, envolveu atividades de forma a construir os fundamentos e bases teóricas para as análises da fase subsequente. Procedeu-se, dessa forma, com a contextualização do tema, inserindo conceitos introdutórios ao entendimento da ameaça abordada na pesquisa.

Ainda nessa etapa, realizou-se a revisão da literatura. Dessa forma, o trabalho utilizou-se de extensa pesquisa bibliográfica de caráter exploratório e descritivo, na qual foram utilizados, em essência, dados secundários, constantes em teses, artigos, livros, periódicos e materiais correlatos (pesquisa bibliográfica). A bibliografia pertinente "oferece meios para definir, resolver, não somente problemas já conhecidos, como também explorar novas áreas em que os problemas não se cristalizaram suficientemente" [97]. Assim, "a pesquisa

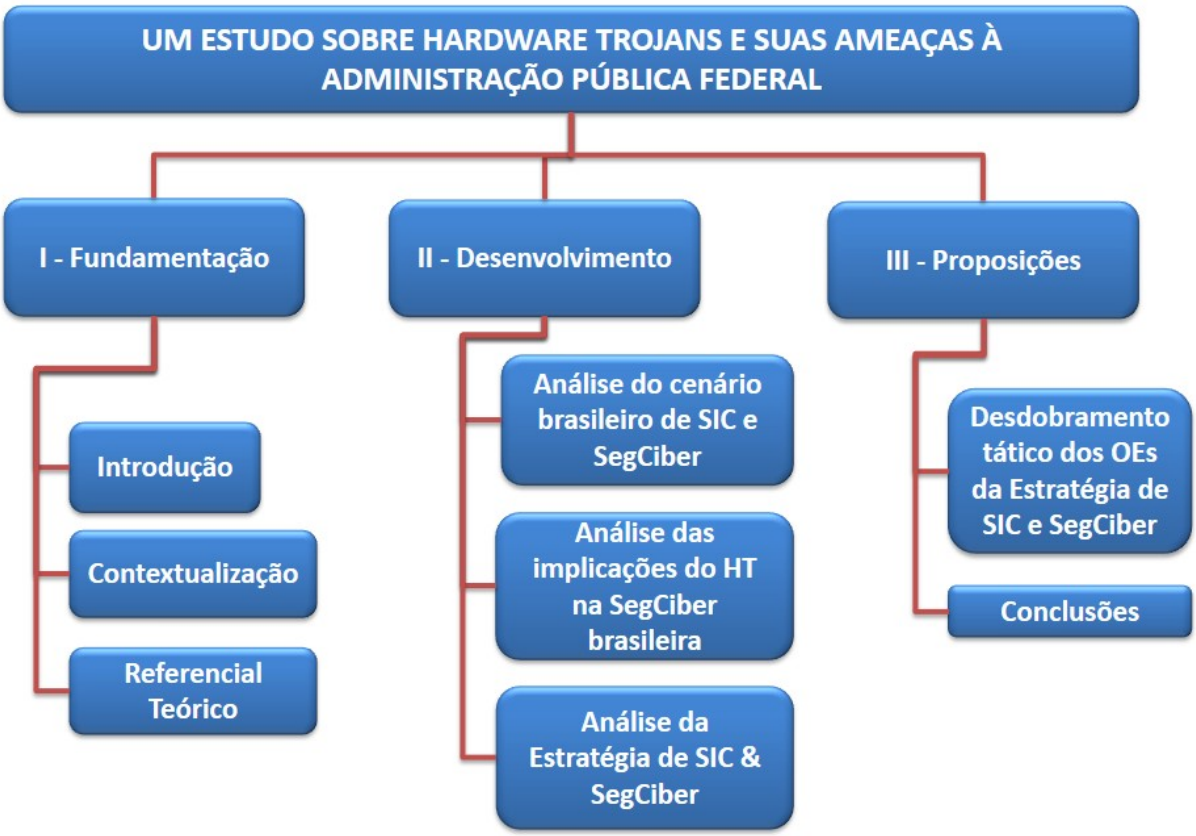

Figura 3.1: Estruturação da metodologia da pesquisa.

bibliográfica não é mera repetição do que já foi dito ou escrito sobre certo assunto, mas propicia o exame de um tema sob novo enfoque ou abordagem, chegando a conclusões inovadoras" [94].

No levantamento de fontes da pesquisa bibliográfica, utilizou-se o enfoque meta-analítico.

A meta-análise surgiu com o objetivo de dotar as revisões de pesquisa com o rigor, a objetividade e a sistematização necessárias para que se constitua o verdadeiro saber científico [98]. Segundo Mariano [33], uma ideia desenvolvida por muitos pesquisadores é a combinação de resultados de estudos independentes para a produção de um fenômeno mais geral de interesse. Esses mesmos autores propuseram um método de revisão, adaptado de Garcia e Ramirez [34], que é composto de sete fases (Figura 3.2, adaptada de Mariano [33]).

3.1.2 Etapa II - Desenvolvimento

Com base nos fundamentos teóricos levantados na etapa anterior, na fase de Desenvolvimento buscou-se a aplicação do conhecimento adquirido na análise da realidade do Estado brasileiro.

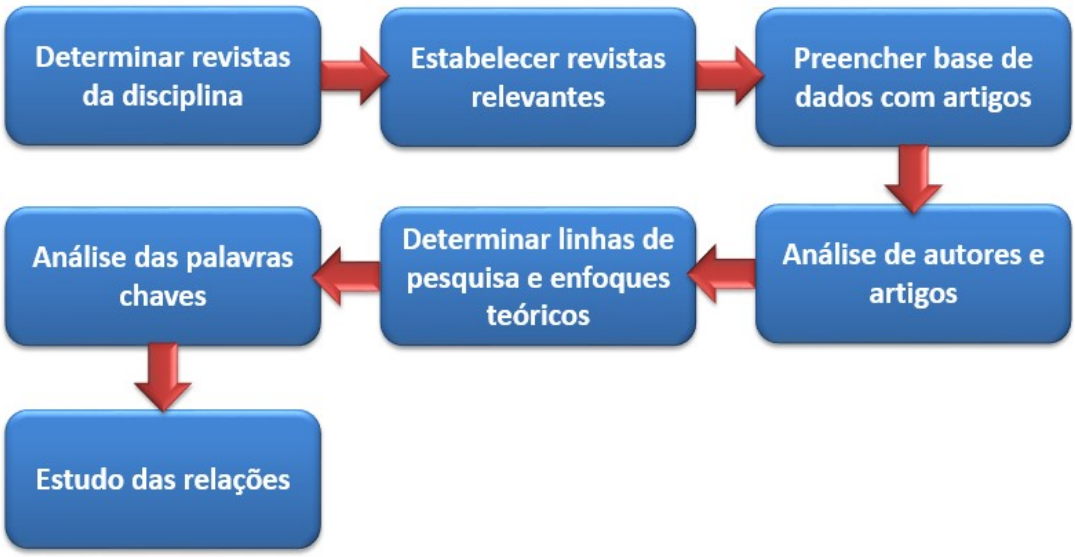

Figura 3.2: Modelo enfoque meta-analítico 7f.

Dessa forma, realizou-se preliminarmente análise do panorama brasileiro em segurança da informação e segurança cibernética, incluindo a forma como o Estado brasileiro se estrutura, do ponto de vista institucional e organizacional, para lidar com os temas.

Após, analisou-se especificamente as implicações do fenômeno hardware Trojan na segurança cibernética do Estado brasileiro.

Por fim, realizou-se análise da Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015 - 2018.

Nessa etapa, a pesquisa documental, envolvendo dados primários, também foi utilizada, notadamente no levantamento do arcabouço legal relacionado às áreas de estudo (leis, decretos, instruções normativas, documentos estratégicos, e assim por diante) e na análise das estruturas institucionais e organizacionais do governo federal brasileiro.

Quanto à abordagem da pesquisa, escolheu-se a abordagem qualitativa, uma vez verificada a escassez de dados numéricos acerca do tema em estudo [94].

3.1.3 Etapa III - Proposições

Quanto à natureza, o presente estudo classifica-se como pesquisa aplicada, entendendo-se como aquela que objetiva gerar conhecimentos para aplicação prática, dirigida à solução de problemas específicos, envolvendo verdades e interesses locais [95].

Assim, na fase propositiva do trabalho, objetivou-se o uso do método indutivo com a finalidade de apontar caminhos possíveis que possam ser considerados pelo governo brasileiro para lidar com o problema.

A fase envolveu ainda o desdobramento, no nível tático, dos objetivos estratégicos presentes na Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015 - 2018, utilizando-se da metodologia BSC para a proposição de Iniciativas Estratégicas, e da metodologia 5W2H para auxílio no desdobramento tático.

Por fim, a presente etapa envolveu a apresentação de conclusões gerais do trabalho.

Capítulo 4

Pesquisa Documental

4.1 Órgãos da Administração Pública Federal no contexto da segurança da informação e da segurança cibernética

Dois campos distintos, embora complementares, são considerados na estruturação dos órgãos federais: a Defesa Cibernética, a cargo do Ministério da Defesa; e a Segurança da Informação e Segurança Cibernética, a cargo da Presidência da República (PR). O presente tópico focará esses últimos.

Na legislação brasileira atual [99] [100] [101] [102] [103], o órgão responsável por coordenar as atividades de segurança da informação e das comunicações no Governo Federal é o Gabinete de Segurança Institucional (GSI).

Em sua missão, o GSI relaciona-se com outros órgãos com atribuições afetas à área de SIC e SegCiber (Figura 4.1, criação do autor).

4.1.1 Conceitos

A partir do estabelecimento do Setor Cibernético, decorrente da aprovação da Estratégia Nacional de Defesa [104], dois campos distintos passaram a ser reconhecidos: a Segurança Cibernética, a cargo da Presidência da República (PR); e a Defesa Cibernética, a cargo do Ministério da Defesa, por meio das Forças Armadas [105].

Na visão do Ministério da Defesa, as ações no Espaço Cibernético deverão ter as seguintes denominações, de acordo com os quatro níveis de decisão (Figura 4.2, retirada da Doutrina Militar de Defesa Cibernética [105]):

No **nível político**, tem-se a Segurança da Informação e Comunicações (SIC) e Segurança Cibernética (SegCiber), coordenadas pela Presidência da República e abrangendo

Figura 4.1: Órgãos da Administração Pública Federal no contexto da SIC e SegCiber.

a Administração Pública Federal direta e indireta, bem como as infraestruturas críticas de informação nacionais [105].

A segurança da informação é a proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento [106].

Os ativos de informação são os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso [1].

A segurança da informação e comunicações, conforme previsto na Instrução Normativa GSI nº 01/2008 [102], engloba ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

Por sua vez, a segurança cibernética é a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas [1].

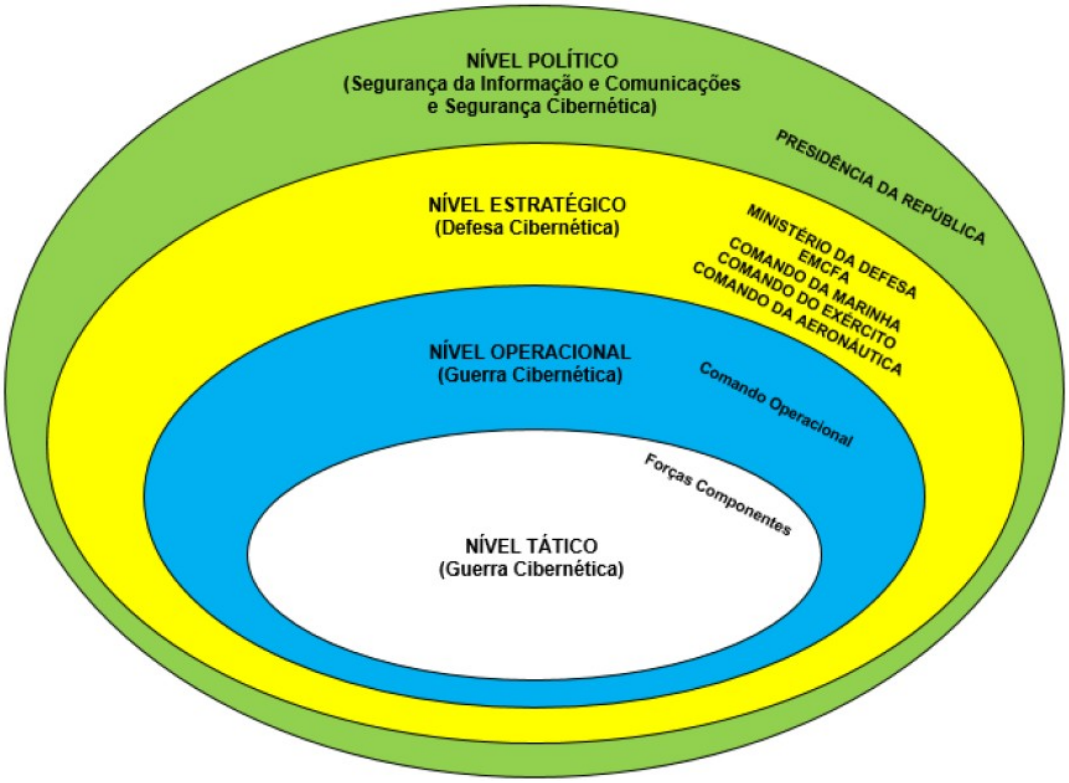

Figura 4.2: Níveis de Decisão no Espaço Cibernético.

As infraestruturas críticas representam 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 [1].

As infraestruturas crítica da informação representam um subconjunto de ativos de informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade [1].

No **nível estratégico**, situa-se a Defesa Cibernética, a cargo do Ministério da Defesa, Estado-Maior Conjunto das Forças Armadas e Comandos das Forças Armadas, interagindo com a Presidência da República e a Administração Pública Federal;

A Defesa Cibernética é o conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente[105].

E, por fim, nos **níveis operacional e tático**, tem-se a Guerra Cibernética, denominação restrita ao âmbito interno das Forças Armadas.

A Guerra Cibernética é entendida como um conjunto de ações para uso ofensivo e defensivo de informações e sistemas de informações para negar, explorar, corromper ou

destruir valores do adversário baseados em informações, sistemas de informação e redes de computadores [107].

A SIC e a SegCiber são a base da Defesa Cibernética e visam assegurar o uso do espaço cibernético, impedindo ou dificultando, em seu âmbito, ações contra os interesses do País e da sociedade [12].

Por fim, define-se os ataques cibernéticos como ações deliberadas com o emprego de recursos da tecnologia da informação e comunicações que visem a interromper, penetrar, adulterar ou destruir redes utilizadas por setores públicos e privados essenciais à sociedade e ao Estado, a exemplo daqueles pertencentes à infraestrutura crítica nacional [10].

4.1.2 Gabinete de Segurança Institucional

O GSI foi criado por meio da Medida Provisória nº 1.911, de 24 de setembro de 1999, que alterava dispositivos da Lei 9.649/1998 [99]. Antes, já foi Casa Militar (1992/Collor), Gabinete Militar (1938/Getúlio Vargas) e Estado-Maior do Governo (1934/Getúlio Vargas).

De acordo com o art. 1º da Lei 9.649/1998 [99], o GSI é um dos chamados órgãos essenciais da Presidência da República, juntamente com a Casa Civil, a Secretaria-Geral e a Secretaria de Comunicação, e seu chefe tem status de Ministro.

Suas competências estão previstas no art. 10 da Medida Provisória nº 782/2017 [100], conforme Tabela 4.1:

Tabela 4.1: Competências do GSI nos termos da MP 782/2017

1	Assistir direta e imediatamente o Presidente da República no desempenho de suas atribuições; especialmente quanto a assuntos militares e de segurança;
2	Analisar e acompanhar questões com potencial de risco, prevenir a ocorrência e articular o gerenciamento de crises, em caso de grave e iminente ameaça à estabilidade institucional;
3	Coordenar as atividades de inteligência federal;
4	Coordenar as atividades de segurança da informação e das comunicações;
5	Zelar, assegurado o exercício do poder de polícia, pela segurança pessoal do Presidente da República, do Vice-Presidente da República e de seus familiares, dos titulares dos órgãos essenciais da Presidência da República pela segurança dos palácios presidenciais e das residências do Presidente da República e do Vice-Presidente da República, e, quando determinado pelo Presidente da República, de outras autoridades federais.

O Decreto nº 9.031/2017 [101], que aprovou a estrutura regimental do GSI, traz as seguintes competências (Tabela 4.2):

Tabela 4.2: Competências do GSI nos termos do Decreto nº 9.031/2017

1	Assessorar direta e imediatamente o Presidente da República no desempenho de suas atribuições;
2	Analisar e acompanhar questões com potencial de risco à estabilidade institucional;
3	Prevenir a ocorrência e articular o gerenciamento de crises em caso de grave e iminente ameaça à estabilidade institucional;
4	Coordenar as atividades: de inteligência federal; e de segurança da informação e das comunicações;
5	Realizar o assessoramento pessoal em assuntos militares e de segurança;
6	Planejar e coordenar viagens presidenciais no País e no exterior, em articulação com o Ministério das Relações Exteriores;
7	Zelar, assegurado o exercício do poder de polícia, pela: segurança pessoal do Presidente da República, do Vice-Presidente da República, e de seus familiares; e pela segurança dos palácios presidenciais e das residências do Presidente da República e do Vice-Presidente da República;
8	Apoiar técnica e administrativamente o funcionamento do Conselho de Defesa Nacional - CDN;
9	Exercer as atividades: de Secretaria-Executiva da Câmara de Relações Exteriores e Defesa Nacional - Creden do Conselho de Governo; e de Órgão Central do Sistema de Proteção ao Programa Nuclear Brasileiro;
10	Realizar o acompanhamento de assuntos pertinentes a: terrorismo e às ações voltadas para a sua prevenção, e intercambiar subsídios para a elaboração da avaliação de risco de ameaça terrorista; e infraestruturas críticas, com prioridade aos que se referem à avaliação de riscos; e
11	Exercer as funções de autoridade nacional de segurança em tratados, acordos ou atos internacionais que envolvam o tratamento e a troca de informação sigilosa.

O GSI operacionaliza as ações de segurança da informação e comunicações e segurança cibernética por meio de seu Departamento de Segurança da Informação e Comunicações (DSIC).

As funções do DSIC estão previstas no art. 11 do Anexo I ao Decreto 9.031/2017 [101], conforme disposto na Tabela 4.3.

A Instrução Normativa nº 01, de 13 de junho de 2008 [102], editada pelo GSI, traz também as seguintes competências ao DSIC (Tabela 4.4):

4.1.3 Comitê Gestor de Segurança da Informação

O Comitê Gestor de Segurança da Informação (CGSI) foi instituído no âmbito do Decreto 3.505/2000 [106], com a atribuição de assessorar a Secretaria-Executiva do Conselho de Defesa Nacional na consecução das diretrizes da Política de Segurança da Informação nos

Tabela 4.3: Competências do DSIC nos termos do Decreto nº 9.031/2017

1	Planejar, coordenar e desenvolver ações de segurança da informação e comunicações, incluídas as de segurança cibernética e de segurança das infraestruturas críticas da informação;
2	Definir normativos e requisitos metodológicos para a implementação de ações de segurança da informação e comunicações, incluídas as de segurança cibernética e de segurança das infraestruturas críticas da informação do Estado;
3	Manter o centro de coordenação de tratamento e resposta a incidentes ocorridos nas redes de computadores da administração pública federal;
4	Avaliar tratados, acordos ou atos internacionais relacionados à segurança da informação, em especial, ao tratamento e à troca de informação sigilosa;
5	Assessorar o Gabinete de Segurança Institucional da Presidência da República no exercício das funções de autoridade nacional de segurança para o tratamento de informação classificada decorrente de tratados, acordos e atos internacionais;
6	Exercer, por meio do Núcleo de Segurança e Credenciamento, na qualidade de Órgão de Registro Central, atividades relacionadas ao credenciamento de segurança e ao tratamento de informação sigilosa;
7	Acompanhar o desenvolvimento da Política Nacional de Segurança da Informação e promover ações para sua implementação; e
8	Exercer outras atribuições que lhe forem determinadas pelo Secretário de Coordenação de Sistemas

órgãos e nas entidades da Administração Pública Federal, bem como na avaliação e análise de assuntos relativos aos objetivos estabelecidos no Decreto.

O CGSI, coordenado pelo GSI, é formado por integrantes de 17 Ministérios (ou órgãos com status de Ministério), indicados pelos titulares de seus respectivos órgãos (ministros, secretários) e designados pelo Ministro do GSI.

São eles (art. 7º do Decreto 3505/2000 [106]): Gabinete de Segurança Institucional (coordenador); Ministério da Justiça; Ministério da Defesa; Ministério das Relações Exteriores; Ministério da Fazenda; Ministério da Previdência Social; Ministério da Saúde; Ministério do Desenvolvimento, Indústria e Comércio; Ministério do Planejamento, Desenvolvimento e Gestão; Ministério das Comunicações; Ministério da Ciência, Tecnologia e Inovação; Casa Civil; Secretaria de Comunicação Social da Presidência da República; Ministério das Minas e Energia; Controladoria-Geral da União; Advocacia-Geral da União; e Secretaria-Geral da Presidência.

A Instrução Normativa nº 01/2008 do GSI [102] traz, em seu art. 4º, as seguintes atribuições do CGSI: Assessorar o GSI no aperfeiçoamento da Gestão de Segurança da Informação e Comunicações da Administração Pública Federal, direta e indireta; e instituir grupos de trabalho para tratar de temas específicos relacionados à segurança da

Tabela 4.4: Competências do DSIC nos termos da IN/GSI 01/2008

1	Planejar e coordenar as atividades de segurança da informação e comunicações na Administração Pública Federal, direta e indireta;
2	Estabelecer normas definindo os requisitos metodológicos para a implementação da Gestão de Segurança da Informação e Comunicações pelos órgãos e entidades da Administração Pública Federal, direta e indireta;
3	Operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da Administração Pública Federal, direta e indireta, denominado CTIR.GOV;
4	Elaborar e implementar programas destinados à conscientização e à capacitação dos recursos humanos em segurança da informação e comunicações;
5	Orientar a condução da Política de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta;
6	Receber e consolidar os resultados dos trabalhos de auditoria de Gestão de Segurança da Informação e Comunicações da Administração Pública Federal, direta e indireta;
7	Propor programa orçamentário específico para as ações de segurança da informação e comunicações.

informação e comunicações.

4.1.4 Conselho de Defesa Nacional

O Conselho de Defesa Nacional é previsto no art. 91 da Constituição Federal [108]. Trata-se de um órgão consultivo à disposição do Chefe de Estado em "assuntos relacionados com a soberania nacional e a defesa do Estado democrático".

O Conselho é presidido pelo PR e dele participam como membros natos: o Vice-Presidente; o Presidente da Câmara dos Deputados; o Presidente do Senado Federal; o Ministro da Justiça; o Ministro de Estado da Defesa; o Ministro das Relações Exteriores; o Ministro do Planejamento; e os comandantes da Marinha, Exército e Aeronáutica.

O §2º do art. 91 da Constituição Federal [108] delegou ao regramento infraconstitucional a organização e o funcionamento do CDN, que foi definido pela Lei 8.183/1991 [109].

Nos termos da lei, compete ao Conselho de Defesa Nacional:

- opinar nas hipóteses de declaração de guerra e de celebração de paz;

- opinar sobre a decretação do estado de defesa[1], do estado de sítio[2] e da intervenção federal[3];
- propor os critérios e condições de utilização das áreas indispensáveis à segurança do território nacional e opinar sobre seu efetivo uso, especialmente na faixa de fronteira e nas relacionadas com a preservação e a exploração dos recursos naturais de qualquer tipo;
- estudar, propor e acompanhar o desenvolvimento de iniciativas necessárias a garantir a independência nacional e a defesa do estado democrático.

O §3º do art. 2º da Lei 8.183/1991 [109] diz que o CDN terá uma Secretaria Executiva para a execução das atividades permanentes necessárias ao exercício de sua competência. No art. 4º, é dito que cabe ao GSI executar tais atividades permanentes. Como já foi abordado, o Chefe do GSI é o Secretário-Executivo do CDN.

Tem-se ainda, nos termos da lei, que as manifestações do Conselho de Defesa Nacional serão fundamentadas no estudo e no acompanhamento dos assuntos de interesse da independência nacional e da defesa do estado democrático, em especial os que se refere:

- à segurança da fronteira terrestre, do mar territorial, do espaço aéreo e de outras áreas indispensáveis à defesa do território nacional;
- quanto à ocupação e à integração das áreas de faixa de fronteira;
- quanto à exploração dos recursos naturais de qualquer tipo e ao controle dos materiais de atividades consideradas do interesse da defesa nacional.

[1]Nos termos do art. 136 da CF/88, o Presidente da República, após ouvir o Conselho da República e o CDN, poderá decretar o estado de defesa "para preservar ou prontamente restabelecer, em locais restritos e determinados, a ordem pública ou a paz social ameaçadas por grave e iminente instabilidade institucional ou atingidas por calamidades de grandes proporções na natureza". Após decretá-lo, o PR enviará ao Congresso Nacional as justificativas para que o legislativo o aprove (por maioria absoluta)

[2]Nos termos do art. 137 da CF/88, o Presidente da República declara o estado de sítio após a autorização do Congresso Nacional por maioria absoluta. O dispositivo é utilizado em duas situações: (1) comoção grave de repercussão nacional ou ocorrência de fatos que comprovem a ineficácia de medida tomada durante o estado de defesa; (2) declaração de estado de guerra ou resposta a agressão armada estrangeira. Observa-se então que o estado de sítio exige prévia autorização do Congresso Nacional, enquanto que no estado de defesa há apenas aprovação posterior

[3]A intervenção federal é uma medida de caráter excepcional e temporário que afasta a autonomia dos estados, Distrito Federal ou municípios. Nos termos do art. 36 da CF/88, a decretação de intervenção federal ocorre nos seguintes casos: (1) quando houver coação contra o Poder Judiciário, para garantir seu livre exercício; (2) quando for desobedecida ordem ou decisão judiciária; (3) quando houver representação do Procurador-Geral da República. A intervenção também deve ser aprovada pelo CN, como no caso do estado de defesa.

4.1.5 Conselho de Governo e a Câmara de Relações Exteriores e Defesa Nacional

O Conselho de Governo integra a Presidência da República como órgão de assessoramento imediato ao PR, conforme prevê o inciso I do §1º do art. 2º da MP 782/2017 [100]. Esse assessoramento se dá por meio de dois níveis de atuação (art. 12) : por meio do Conselho propriamente dito; e por meio das Câmaras do Conselho de Governo, a serem criadas "em ato do Poder Executivo federal, com a finalidade de formular políticas públicas setoriais cujo escopo ultrapasse as competências de um único Ministério".

Uma dessas câmaras é a Câmara de Relações Exteriores e Defesa Nacional (CREDEN), criada por meio do Decreto 4.801/2003 [110] com a finalidade de formular políticas públicas e diretrizes de matérias relacionadas com a área das relações exteriores e defesa nacional do Governo Federal, além de aprovar, promover a articulação e acompanhar a implementação dos programas e ações estabelecidos, no âmbito de ações cujo escopo ultrapasse a competência de um único Ministério.

Tais ações, nos termos do art. 1º, englobam, dentre outros, os seguintes assuntos: atividade de inteligência; segurança das infraestruturas críticas, incluindo serviços; segurança da informação; e segurança cibernética.

O Ministro do GSI, conforme já abordado, exerce as funções de Secretário-Executivo da CREDEN e a preside.

Atualmente, a CREDEN é integrada pelos seguintes Ministros de Estado (art. 2º do Decreto 4.801/2003 [110]): Chefe do GSI (Presidente do Conselho); Chefe da Casa Civil; Ministro da Justiça; Ministro da Defesa; Ministro das Relações Exteriores; Ministro do Planejamento; Ministro do Meio Ambiente; Ministro da Ciência e Tecnologia; Ministro da Fazenda; Chefe da Secretaria de Assuntos Estratégicos/PR (a SAE foi extinta em 2015 – o decreto está desatualizado); Ministro da Saúde; Ministro das Comunicações; Ministro da Integração Nacional; Ministro das Minas e Energia; e Ministro dos Transportes.

Além disso, são convidados a participar das reuniões, em caráter permanente, os Comandantes da Marinha, do Exército, da Aeronáutica e o Chefe do Estado-Maior Conjunto das Forças Armadas.

4.1.6 Agência Brasileira de Inteligência

A Agência Brasileira de Inteligência (ABIN) foi criada por meio da Lei 9.883/1999 [32] como órgão central do Sistema Brasileiro de Inteligência (SISBIN)[4].

[4]Nos termos do art. 2º da Lei 9.883/1999, os órgãos e entidades da Administração Pública Federal que, direta ou indiretamente, possam produzir conhecimentos de interesse das atividades de inteligência, em especial aqueles responsáveis pela defesa externa, segurança interna e relações exteriores, constituirão o Sistema Brasileiro de Inteligência, na forma de ato do Presidente da República.

O SISBIN integra as ações de planejamento e execução das atividades de inteligência do País, com a finalidade de fornecer subsídios ao Presidente da República nos assuntos de interesse nacional. Ainda, é responsável pelo processo de obtenção, análise e disseminação da informação necessária ao processo decisório do Poder Executivo, bem como pela salvaguarda da informação contra o acesso de pessoas ou órgãos não autorizados.

Nos termos da Lei 9.883/1999 [32], a inteligência é entendida como a atividade que objetiva a obtenção, análise e disseminação de conhecimentos dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado. Caracteriza-se ainda pela identificação de fatos e situações que representem obstáculos ou oportunidades aos interesses nacionais. O levantamento e o processamento de dados e a análise de informações ajudam os decisores governamentais a superar obstáculos ou a aproveitar oportunidades [111].

Por outro lado, a contra-inteligência engloba as atividades que objetivam neutralizar a inteligência adversa. Tem como atribuições a produção de conhecimentos e a realização de ações voltadas para a proteção de dados, conhecimentos, infraestruturas críticas – comunicações, transportes, tecnologias de informação – e outros ativos sensíveis e sigilosos de interesse do Estado e da sociedade [111].

À ABIN compete (Tabela 4.5):

Tabela 4.5: Competências do ABIN nos termos da Lei nº 9.883/1999

1	Planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência do País;
2	Planejar e executar ações, inclusive sigilosas, relativas à obtenção e análise de dados para a produção de conhecimentos destinados a assessorar o Presidente da República;
3	Planejar e executar a proteção de conhecimentos sensíveis, relativos aos interesses e à segurança do Estado e da sociedade;
4	Avaliar as ameaças, internas e externas, à ordem constitucional;
5	Promover o desenvolvimento de recursos humanos e da doutrina de inteligência, e realizar estudos e pesquisas para o exercício e aprimoramento da atividade de inteligência.

A ABIN subordina-se ao GSI, conforme art. 11 da Medida Provisória nº 782, de 31 de maio de 2017 [100].

A agência trabalha internamente com a inteligência cibernética. Sua Secretaria de Planejamento e Gestão é responsável por planejar, coordenar, supervisionar, controlar e avaliar as atividades de desenvolvimento científico e tecnológico, de Inteligência cibernética, de telecomunicações e de eletrônica, dentre outras [112].

Em 2016, com a publicação da Política Nacional de Inteligência [10], a ABIN definiu como uma de suas diretrizes a expansão da capacidade operacional da Inteligência no espaço cibernético.

Através de seu Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (Cepesc), a ABIN desenvolve pesquisas científicas e tecnológicas aplicadas a projetos e soluções de segurança das comunicações e Inteligência cibernética; a projetos de implementação de algoritmos criptográficos de Estado em soluções voltadas para a segurança da informação e das comunicações; e apoia a Secretaria-Executiva do Conselho de Defesa Nacional (ou seja, o GSI) nas atividades de caráter científico e tecnológico relacionadas à segurança da informação e à segurança cibernética [112].

4.1.7 Comando de Defesa Cibernética do Exército Brasileiro

A Estratégia Nacional de Defesa (END) foi aprovada por meio do Decreto nº 6.703, de 18 de dezembro de 2008 [104]. O documento estabelece três setores estratégicos e essenciais para a defesa nacional: o espacial; o nuclear; e o cibernético.

O documento delegou à Marinha do Brasil a gerência do programa nuclear; ao Exército Brasileiro (EB), a liderança da defesa cibernética em território nacional; e à Força Aérea, o programa espacial (Figura 4.3, criação do autor).

Figura 4.3: Setores Estratégicos - Defesa Nacinal.

Antes de estabelecer o Comando de Defesa Cibernética, com a missão de coordenar e integrar as ações de Defesa Cibernética, o Exército criou o Centro de Defesa Cibernética (CDCIBER) por meio da Portaria nº 666, de 4 de agosto de 2010 [113].

O Centro estava inicialmente ligado ao Departamento de Ciência e Tecnologia (DCT), órgão responsável por atividades científicas, tecnológicas e de inovação do EB.

Paralelamente à publicação da Portaria 666, publicou-se Portaria nº 667 [114], que ativou o Núcleo do Centro de Defesa Cibernética (NuCDCiber), também vinculado ao DCT, cuja responsabilidade seria a implantação do CDCiber.

A estrutura foi formalizada com subordinação ao DCT por meio do Decreto nº 7.809/2012 [115], que alterou o Decreto nº 5.751/2006 [116], que trata da estrutura do Comando do Exército. Mais tarde, com a publicação do Decreto nº 8.491/2015 [117], que também atualizou o Decreto nº 5.751/2006, o Centro de Defesa Cibernética saiu da estrutura do DCT e foi definido como órgão de assistência direta e imediata ao Comandante do Exército, nos termos da alínea "f" do inciso III do art. 4º do Decreto nº 5.751/2006.

Em 27/10/2014, a Portaria nº 2777 do Ministério da Defesa [118] aprovou as diretrizes para a "implantação de medidas visando à potencialização da Defesa Cibernética Nacional". Assim, foram definidas duas iniciativas: a criação, na estrutura do EB, do Comando de Defesa Cibernética (ComDCiber), que contará, na forma da legislação, com o exercício de militares das três Forças Armadas, cabendo ao Estado Maior Conjunto das Forças Armadas as atividades de coordenação nos casos de operações conjuntas, especificando-se, em atos próprios, os aspectos inerentes ao controle operacional; e a criação, também na estrutura do EB, da Escola Nacional de Defesa Cibernética (ENaDCiber).

Como é de praxe no Exército, a criação das estruturas definitivas é precedida pela instalação de "núcleos". Dessa forma, a mesma portaria incumbiu ao EB a criação de dois núcleos: o Núcleo do Comando de Defesa Cibernética (NuComDCiber), subordinado ao Centro de Defesa Cibernética (CDCiber), dotado de pessoal e infraestrutura para os trabalhos de implantação do Comando de Defesa Cibernética (ComDCiber); e o Núcleo da Escola Nacional de Defesa Cibernética (NuENaDCiber), subordinado ao Centro de Defesa Cibernética (CDCiber), dotado de pessoal e infraestrutura para os trabalhos de implantação da (ENaDCiber);

Em 21/07/2015, como desdobramento da Portaria nº 2777, o EB inaugurou os dois núcleos no Comando Militar do Planalto, localizado no Setor Militar Urbano (próximo ao QG/EB): o NuComDCiber e o NuENaDCiber.

As estruturas definitivas foram formalizadas por meio do Decreto nº 8.913/2016 [119], que alterou o Decreto nº 5.751/2006, que trata da estrutura do Comando do Exército. Com a atualização, o Centro de Defesa Cibernética (CDCiber) deixou de existir, e o

Comando de Defesa Cibernética (ComDCiber) passou a compor a estrutura do Departamento de Ciência e Tecnologia (DCT).

4.2 Implicações do fenômeno hardware Trojan em questões relativas à segurança cibernética brasileira

Conforme descrito na seção anterior, o planejamento, a coordenação e o desenvolvimento de ações de segurança da informação e comunicações, incluídas as de segurança cibernética e de segurança das infraestruturas críticas da informação [101], é uma das competências atribuídas ao GSI, órgão integrante da estrutura da Presidência da República.

É fato que o país vem evoluindo na área, tanto na estruturação de seus órgãos, como na criação de regulamentações no setor. Conforme apontado em Brasil [12], os temas ligados à segurança da informação vêm se caracterizando cada vez mais como funções estratégicas de Estado, sendo essenciais à manutenção e preservação tanto das infraestruturas críticas de um país, tais como Energia, Transporte, Telecomunicações, Águas, Finanças, a própria Informação, entre outras, quanto dos direitos individuais, em especial da privacidade, e da soberania.

O fenômeno hardware trojan está fortemente relacionado com questões ligadas à soberania e espionagem entre países. Como já abordado anteriormente, dentre as ações possíveis implementadas pelo agente malicioso está o vazamento de informações sensíveis que trafegam nos sistemas infectados. Além disso, considerando a grande complexidade envolvida na implementação do hardware trojan, é pouco provável que a ameaça se origine nas mãos de um cibercriminoso comum, como observado nos diversos tipos de *malware* (do inglês *Malicious Software*, qualquer código malicioso implementado via software [4]). Assim, se a espionagem entre nações é uma realidade, espera-se que os países criem mecanismos capazes de lidar com o problema que envolve, muitas das vezes, questões de privacidade e soberania.

Em meados de 2013, o mundo assistiu atônito às revelações feitas por Edward Snowden, um ex-técnico da CIA – a agência de inteligência norte-americana, sobre supostas ações de espionagem dos EUA em vários países, aliados ou não.

A revelação de documentos foi feita de forma paulatina, a princípio divulgados pelos periódicos The Guardian e Washington Post. No entanto, não tardou para que aparecessem indícios, dentre os documentos vazados, de que os americanos também haviam espionado e-mails, ligações telefônicas e dados digitais no Brasil, incluindo dados ligados à Presidente da República, Dilma Vana Rousseff.

Pressionado pela mídia e por setores da sociedade, o Governo veio a instalar, em julho de 2013, uma Comissão Parlamentar de Inquérito (CPI) no Senado para apurar as denúncias. A CPI é um instituto previsto na Constituição Federal, e goza de poderes de investigação próprios das autoridades judiciais [108]. À época, havia indícios de que equipes das agências de inteligência americana vinham, inclusive, atuando em solo nacional, com base própria na Capital da República, ferindo princípios primordiais de soberania do país [120].

Quase um ano depois, em abril de 2014, a CPI apresentou seu relatório final, abordando conclusões e recomendações. Dentre aquelas, destaca-se a constatação da vulnerabilidade do país diante da espionagem proveniente de outros Estados.

Ainda no ano de 2013, em resposta ao clima de insegurança que já se instalara em diversos setores do país, o governo brasileiro promulgou o Decreto nº 8.135/2013 [11], que dispôs sobre as comunicações de dados da administração pública federal. Segundo o normativo, os programas e equipamentos destinados às atividades de comunicação de dados na administração pública federal deverão ter características que permitam auditoria para fins de garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações [11]. O Decreto não abordou detalhes dessa auditoria, deixando a tarefa para a legislação infralegal.

Em 2014, uma portaria envolvendo o então Ministério do Planejamento, Orçamento e Gestão (hoje Ministério do Planejamento, Desenvolvimento e Gestão), o Ministério das Comunicações e o Ministério da Defesa – a Portaria nº 141 [121], complementou os termos do Decreto.

Conforme previsto no art. 13 da Portaria, a auditoria deve ser conduzida pelo órgão ou entidade contratante ou por instituição credenciada pelo governo federal para tal finalidade [121].

Ainda segundo o regulamento, o governo deverá exigir, no mínimo, a possibilidade de abertura do código fonte no caso de programas para comunicação de dados; e de *firmware* e sistemas operacionais, no caso de equipamentos para comunicação de dados.

Lembrando o fato de que as implementações de HT permanecem ocultas nos sistemas infectados, é razoável considerar a hipótese de ataques de HT dirigidos ao governo brasileiro, que somente em 2016 gastou mais de R$ 6 bilhões em tecnologia da informação, com previsão de desembolsos da ordem de R$ 7,8 bilhões em 2017 [122]. Não obstante a potencial ameaça, o que se observa na legislação é uma abordagem ainda focada nas comunicações e no software como pontos de falha da segurança cibernética. Não há uma referência, ao menos de forma direta, à questão do hardware Trojan.

De fato, como bem pontuou Villasenor [26], toda a atenção prestada, em anos recentes, à segurança cibernética ainda repousa seu foco no software, não só em termos de

técnicas empregadas, como também na expertise de pessoas e empresas ligadas à área. Não obstante, diversos países têm se movimentado para estruturar áreas dedicadas a essas e outras questões de segurança cibernética, como o governo australiano que, por meio de seu Departamento de Defesa, vem publicando diversos estudos sobre a temática do hardware trojan, a exemplo de [31] e [123].

No Brasil, a criação do Comando de Defesa Cibernética, conforme descrito na seção anterior, vem ao encontro dessa tendência e buscou estabelecer no país capacidade de coordenação e integração das atividades do setor cibernético.

Não obstante, a Administração Pública Federal permanece exposta a ameaças possíveis com a implementação de HT em equipamentos eventualmente adquiridos pelo Governo, as quais destacam-se:

- Vazamento de informações sigilosas do Governo Federal [31] [124]; [21] [52] [125] [27] [51] [44] [61] [126] [45] [28];
- Ataques de indisponibilidade em sistemas críticos [45] [31] [127] [51] [42] [44] [59];
- Alteração de funcionalidade em sistemas [51] [46];
- Criação de falhas e mal-funcionamento em equipamentos e sistemas [45]; [28] [52] [51].

4.3 A Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015 - 2018

Desde 2007, o Tribunal de Contas da União (TCU), órgão auxiliar do controle externo [108], vem coletando informações sobre a situação da governança de tecnologia da informação (TI) junto às organizações que integram a estrutura da Administração Pública Federal (APF).

Em 2014, auditorias foram realizadas em diversos órgãos e entidades da Administração Pública Federal com o objetivo de avaliar a implementação dos controles de TI informados em resposta ao levantamento do perfil de governança de TI de 2012, bem como verificar a implementação de controles e processos de governança e gestão de TI para assegurar a entrega de resultados de TI alinhados aos objetivos de negócio das instituições, gerenciando os riscos de TI existentes [128].

Como resultado dos trabalhos do Acórdão TCU nº 3051/2014, do Plenário [128], o Tribunal destacou que a segurança da informação permanecia sendo objeto de preocupa-

ção, apresentando baixa conformidade das organizações para com os normativos e boas práticas aplicáveis ao tema.

No mesmo ano, por meio do Acórdão TCU nº 3117/2014, do Plenário [129], a Corte de Contas observou que a segurança da informação tem sido objeto de preocupação em todos os levantamentos anteriores por causa da baixa conformidade das organizações em relação aos normativos e às boas práticas aplicáveis.

No mesmo processo, a Corte de Contas concluía que a despeito da evolução identificada no período 2012 a 2014, o nível de adoção das práticas apresentadas está muito distante do esperado, situação que revela a existência de lacunas na coordenação e na normatização da gestão corporativa da segurança da informação, expondo a APF a diversos riscos, como indisponibilidade de serviços e perda de integridade de informações.

Diante de todo o cenário observado em seus levantamentos de auditoria, o TCU acabou recomendando, por meio do Acórdão TCU nº 3051/2014, do Plenário [128], que o GSI promovesse a elaboração (e acompanhamento periódico) de um planejamento abrangendo a estratégia geral de segurança da informação para o setor sob sua jurisdição, envolvendo não somente a tecnologia da informação, mas também os demais segmentos relacionados à proteção das informações institucionais.

Em resposta à recomendação do Tribunal, em 26 de dezembro de 2014, o GSI instituiu, por meio do Boletim Interno GSI/PR nº 52 [12], um Grupo Técnico formado por membros de seu Departamento de Segurança das Informações e Comunicações (DSIC), com o objetivo de elaborar minuta da Estratégia de Segurança da Informação e Comunicações da Administração Pública Federal.

A Estratégia então foi elaborada e homologada em 11 de maio de 2015, por meio de portaria do Conselho de Defesa Nacional [130]. Trata-se de instrumento de apoio ao planejamento estratégico governamental que complementa a Instrução Normativa GSI/PR 01/2008 [102] e reúne um conjunto de objetivos estratégicos e metas para o quadriênio 2015-2018. Visa a busca da excelência da Segurança da Informação e Comunicações (SIC) e da Segurança Cibernética (SegCiber) no âmbito da Administração Pública Federal (APF) do País, contemplando relevantes aspectos, dada a complexidade e a dinâmica de tais temas no cenário atual, nacional e mundial [12].

O documento objetiva ainda apresentar as diretrizes estratégicas para o planejamento de segurança da informação e comunicações e de segurança cibernética no âmbito da APF, articulando e coordenando esforços dos diversos atores envolvidos, de forma a atingir o aprimoramento da área no Governo e a mitigação dos riscos aos quais encontram-se expostas as organizações e a sociedade [12].

A missão declarada foi a de fortalecer a política e o planejamento de segurança da informação e comunicações e de segurança cibernética na Administração Pública Federal,

visando assegurar e defender os interesses do Estado e da sociedade para a preservação da soberania nacional.

Como visão de futuro, o GSI buscará fazer com que a Estratégia seja reconhecida como instrumento de planejamento governamental para a excelência em segurança da informação e comunicações e em segurança cibernética na Administração Pública Federal.

Os princípios norteadores da Estratégia envolveram os conceitos dispostos na Tabela 4.6.

A estratégia se utilizou, com adaptações ao cenário público, da metodologia de planejamento e gestão estratégica Balanced Scorecard (BSC).

Conforme visto no Capítulo 2, o BSC define as chamadas "perspectivas", eixos de atuação sob as quais o desempenho institucional é medido de forma equilibrada. A Estratégia do GSI trabalhou com quatro perspectivas, a saber: Orçamentária; Aprendizagem, Crescimento e Inovação; Governo; e Resultados para a Sociedade.

Nos termos da descrição metodológica, o documento define a perspectiva Orçamentária como de natureza estruturante, referindo-se ao aporte contínuo e adequado de recursos do orçamento federal para que se viabilize as ações necessárias ao alcance dos objetivos propostos nessa Estratégia; a perspectiva Aprendizagem, Conhecimento e Inovação, também de natureza estruturante, envolvendo o investimento em capital humano, abrangendo ações de sensibilização, conscientização, treinamento, capacitação e especialização nas áreas de SIC e de SegCiber, como forma de preparar os agentes públicos para promover mudanças e viabilizar a consecução dos objetivos propostos na Estratégia; a perspectiva Governo, englobando os processos internos, a legislação, as articulações, as competências institucionais, as estruturas governamentais e tudo o mais que envolva as intra e inter-relações da APF com os demais atores, no alcance dos objetivos; e, por fim, a perspectiva Resultados para a Sociedade, representando a finalidade precípua da ação Estatal – a de direcionar sua conduta sempre visando os interesses e demandas sociais, englobando as ações em SIC e SegCiber que resultem em benefícios para a sociedade, tais como proteção da privacidade, transparência e salvaguarda dos ativos de informação sigilosos [12].

A partir das perspectivas, foram elaborados dez objetivos estratégicos e 38 (trinta e oito) metas para o quadriênio 2015-2018.

A Figura 4.4 mostra o Mapa Estratégico instituído no âmbito da Estratégia de SIC e SegCiber [12], no qual são dispostos os dez objetivos estratégicos ao longo das quatro perspectivas, conforme metodologia prevista no BSC.

O Mapa Estratégico dispõe os objetivos em uma relação de causa e efeito, demonstrando um caminho para se chegar aos resultados almejados. Ou seja, é preciso assegurar recursos suficientes no orçamento, de forma que se invista em aprendizagem, capacitação e inovação, dando condições para que os atores de Governo envolvidos promovam as melho-

Tabela 4.6: Princípios Norteadores da Estratégia de SIC e SegCiber

Órgão Central	contribuir com o estabelecimento de um órgão central e de um sistema nacional, objetivando a coordenação executiva, o acompanhamento e a avaliação da implantação e execução da Política Nacional de SIC e SegCiber.
Governança	contribuir com a definição de um modelo de governança sistêmica de SIC e de SegCiber, de amplo alcance e cobertura para uma conexão forte entre os múltiplos atores, em nível nacional
Política Nacional	contribuir com a formulação da Política Nacional de Segurança da Informação e Comunicações e de Segurança Cibernética
Capacidade de posicionamento e de respostas da Nação	contribuir com a criação de uma robusta capacidade de posicionamento e de respostas da Nação frente às potenciais quebras de segurança e ameaças cibernéticas, fortalecendo a alocação de recursos financeiros, tecnológicos e humanos
Comprometimento da Alta Administração	envolver a Alta Administração dos órgãos e entidades da Administração Pública Federal em relação às diretrizes e ações de SIC e de SegCiber no âmbito de suas atuações
Marcos Legais	colaborar para o aprimoramento e atualização dos marcos legais em SIC e SegCiber
Articulação e Parcerias	garantir que a SIC e a SegCiber estejam contempladas em termos, acordos, contratos e instrumentos firmados entre a APF e setores públicos ou privados, nacionais ou internacionais
Soberania Nacional	reconhecer as áreas de SIC e de SegCiber como estratégicas para a soberania nacional, garantindo recursos contínuos e adequados
Cooperação	promover a cooperação nacional e internacional, visando trocas de experiências e o fortalecimento dos temas de SIC e de SegCiber no âmbito da APF e com setor produtivo e academia
Integração	fomentar e fortalecer ações conjuntas visando à integração entre as áreas de SIC e de SegCiber com outras áreas que atuam no espaço cibernético
Resiliência	contribuir com o aumento da capacidade de resiliência dos ativos de informação e das infraestruturas críticas

rias necessárias nas instituições, nas estruturas e nos processos da gestão governamental e das políticas públicas, derivando na entrega de resultados efetivos para a sociedade e na melhoria do próprio Estado [12].

A Estratégia declarou dez objetivos, dispostos na Tabela 4.7.

Conforme definição do documento, tais objetivos representam forças motrizes para o cumprimento da missão e o alcance da visão de futuro da mesma, estando alinhados aos

Tabela 4.7: Objetivos Estratégicos dispostos na Estratégia de Segurança da Informação e Comunicações e Segurança Cibernética da Administração Pública Federal

OE-I	Institucionalizar o tema de SIC e de SegCiber no planejamento e orçamento federal
OE-II	Garantir continuamente o aprimoramento do quadro de pessoal da APF em SIC e SegCiber, de forma qualitativa e quantitativa
OE-III	Garantir continuamente a pesquisa, o desenvolvimento e a inovação em SIC e SegCiber na APF
OE-IV	Instituir modelo de governança sistêmica de sic e de SegCiber na APF, com coordenação executiva, acompanhamento e avaliação do órgão central (GSI/PR)
OE-V	Alinhar o planejamento de SIC e de SegCiber ao planejamento estratégico dos órgãos e entidades da APF
OE-VI	Ampliar e fortalecer ações colaborativas em SIC e SegCiber com a academia, setores público, privado e terceiro setor, no país e no exterior
OE-VII	Elevar o nível de maturidade de SIC e de SegCiber na APF
OE-VIII	Reforçar a SIC e a SegCiber como alta prioridade na agenda de governo
OE-IX	Valorizar e ampliar ações que fortaleçam a segurança das infraestruturas críticas da informação
OE-X	Promover mecanismos de conscientização da sociedade sobre SIC e SegCiber

princípios norteadores e valores propostos na Estratégia [12].

Quanto às metas, foram declaradas 38 distribuídas ao longo do quadriênio 2015-2018, conforme lista constante no Anexo I.

Tendo em vista a natureza transversal dos Objetivos Estratégicos de SIC e de SegCiber, as metas foram construídas a partir de uma visão holística, ou seja, considerando a Estratégia como um todo, não se vinculando necessariamente cada meta a um único objetivo estratégico [12].

Da análise das metas construídas na estratégia, percebe-se que são desdobramentos táticos dos objetivos estratégicos. Ou seja, a partir da definição, no nível macro, estratégico, sobre o que fazer - conforme declarado nos objetivos estratégicos da Estratégia -, o documento buscou definir ações de forma a contribuir para o alcance dos objetivos Estratégicos como um todo, o que chamou de "meta". Tais metas não foram vinculadas a objetivos específicos.

Conforme já visto no Capítulo 2, na metodologia do BSC, metas são níveis desejados de performance para cada indicador . Estes, por sua vez, são mecanismos utilizados para acompanhar e medir a performance organizacional [84].

Assim, tecnicamente, o que a Estratégia declarou como "meta", para o BSC, a rigor, seriam "iniciativas estratégicas", ou seja, projetos com data de início e fim que visam transformar em ação os objetivos organizacionais [83].

Figura 4.4: Estratégia de SIC e SegCiber: Mapa Estratégico.

Capítulo 5

Elaboração de Propostas

5.1 Propostas de Desdobramentos Táticos dos Objetivos Estratégicos definidos na Estratégia de SIC e de SegCiber

Não há dúvidas de que ações efetivas de prevenção e combate às práticas maliciosas no uso da tecnologia da informação e comunicação são necessárias, e o Governo brasileiro vem formalmente declarando tal necessidade. No entanto, ainda existem lacunas entre necessidades declaradas (e reconhecidas), e as respectivas ações efetivas.

Como bem pontuou Villasenor [26], frequentemente esperamos as catástrofes para impulsionar as mudanças. No entanto, uma vez que os casos envolvendo ataques cibernéticos por meio de hardware Trojan ainda não são publicamente conhecidos ou expostos [20] [49], é difícil impulsionar grandes esforços para lidar com o problema.

Não obstante, considerando o importante papel desempenhado pelos circuitos integrados nos mais diversos sistemas críticos de um país, há boas razões para ser proativo, quando o assunto diz respeito à segurança do hardware [26].

Este trabalho teve como objetivo geral a proposição de desdobramentos no nível tático dos Objetivos Estratégicos definidos na Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal, e teve foco no contexto da segurança cibernética.

Dessa forma, a partir da análise da Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal, e tendo como panorama as questões envolvendo a ameaça do hardware Trojan e suas implicações no contexto da segurança cibernética, serão propostas iniciativas estratégicas a serem eventualmente contempladas na nova Estratégia, de forma que o Brasil possa iniciar esforços para lidar com o problema.

Conforme foi visto no Capítulo 4, a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015 - 2018, publicada em 2015, utilizou, com adaptações, a consagrada metodologia de planejamento e gestão estratégica denominada Balanced Scorecard (BSC).

O BSC cria um sistema que permite o acompanhamento do alcance dos objetivos por meio de indicadores, metas e iniciativas estratégicas. O documento do GSI contemplou apenas as iniciativas estratégicas (que chamou de metas, conforme foi observado no Capítulo 4), trinta e oito no total, que foram distribuídas ao longo do quadriênio 2015/2018 e foram construídas a partir de uma visão holística, ou seja, considerando a Estratégia como um todo, não se vinculando necessariamente cada meta (iniciativa estratégica) a um único objetivo estratégico.

Esse capítulo objetiva a proposição de iniciativas estratégicas que possam ser contempladas em futuras revisões da Estratégia de SIC e SegCiber, de forma a abordar as questões envolvendo o hardware Trojan.

Partiu-se da premissa de que os objetivos estratégicos definidos na Estratégia são abrangentes o bastante para não necessitarem, a princípio, de revisão. Ademais, como o documento trata da segurança da informação e comunicações e da segurança cibernética, e seus objetivos foram construídos dentro desses pilares temáticos, e sendo a segurança cibernética área afeta ao tema em estudo (hardware Trojan), é razoável supor que ações táticas relacionadas ao tema da pesquisa possam se relacionar a um ou mais objetivos estratégicos já declarados pelo documento do GSI.

Na proposição das iniciativas estratégicas, será utilizada a metodologia 5W2H, instrumento útil na elaboração de planos de ação, pois permite a definição de responsabilidades, métodos, prazos, objetivos e recursos associados [92]. A dimensão "como"(how?) prevista na metodologia abordará ações possíveis de implementação, sem a pretensão de esgotar todas as possibilidades de ações que contribuam para a iniciativa.

As iniciativas estratégicas propostas encontram-se listadas na Tabela 5.1 e serão detalhadas separadamente. Para a proposição de tais iniciativas, cada Objetivo Estratégico declarado na Estratégia de SIC e SegCiber foi comparado com possibilidades de ação no âmbito do tema HT, utilizando-se do conhecimento estruturado por meio da revisão da literatura. Portanto, cada iniciativa estratégica proposta será fundamentada com artigos, pesquisas, referenciais normativos ou estudos que trataram do assunto.

A exceção da iniciativa proposta IE1, que baseou-se na "meta M-XV"da Estratégia de SIC e SegCiber, todas as outras são proposições novas. A iniciativa foi adaptada para que se aborde, em mais detalhes, as atividades possíveis no âmbito daquela iniciativa, considerando o contexto do hardware Trojan. De fato, a metodologia 5W2H permite o levantamento de atividades (*how*?) e recursos (*how much*?).

Tabela 5.1: Iniciativas Estratégicas propostas a partir dos Objetivos Estratégicos e perspectivas da Estratégia de SIC e SegCiber

IE1	Formalizar parceria com Escolas de Governo para inserção de cursos e/ou disciplinas de SIC e SegCiber.
IE2	Estabelecer respaldo normativo e jurídico para auditoria de hardware adquirido pelo Governo.
IE3	Fomentar a indústria doméstica de circuitos integrados.
IE4	Estabelecer, em nível nacional, capacidade de coordenação de respostas rápidas a um ataque de HT.
IE5	Criar meios de estabelecer um programa de confiança na fabricação de circuitos integrados.

A Figura 5.1 (criação do autor) representa uma visão esquemática das iniciativas propostas, e suas relações com as perspectivas do BSC e respectivos objetivos estratégicos utilizados na Estratégia de SIC e SegCiber.

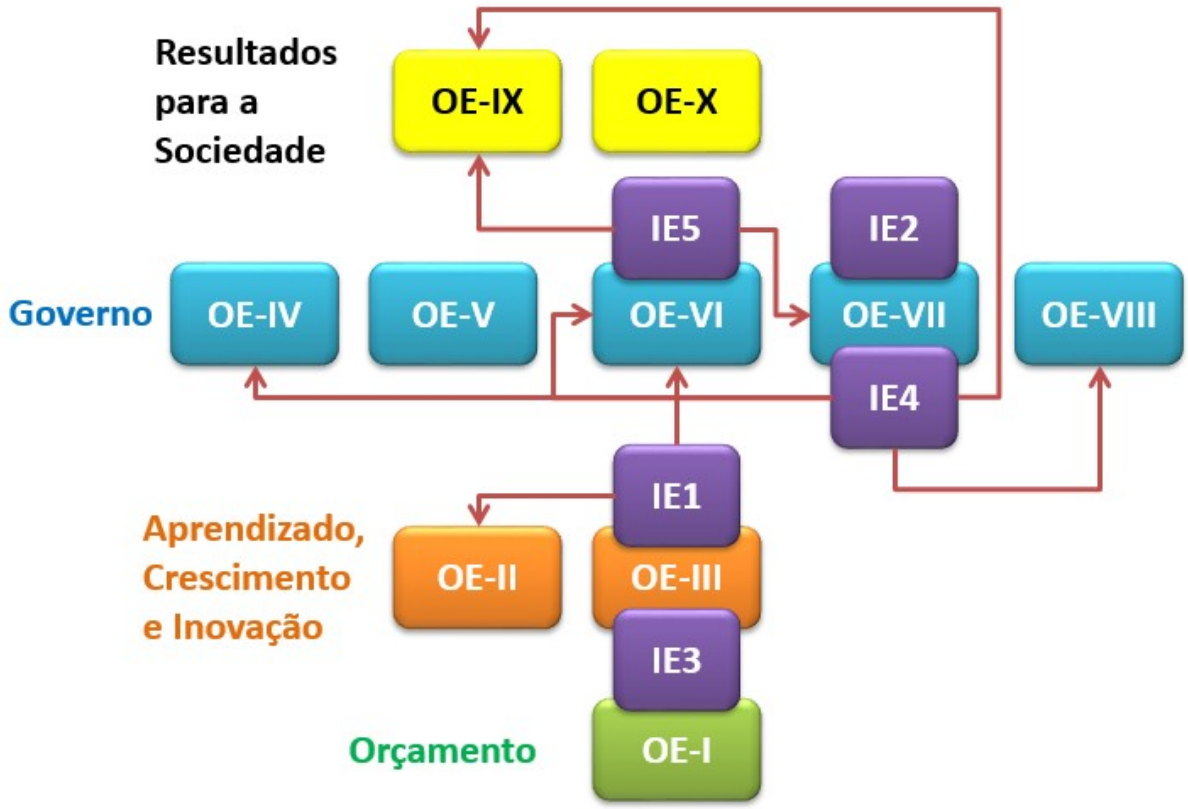

Figura 5.1: Relação entre Iniciativas Estratégicas (IE) propostas e os Objetivos Estratégicos (OE) declarados na Estratégia de SIC e SegCiber.

As iniciativas foram dispostas, propositalmente, sobre os objetivos aos quais estejam

diretamente ligadas (e para os quais haja contribuição direta da iniciativa na consecução do objetivo). No entanto, considerando que as iniciativas foram construídas sob um enfoque de atuação transversal e holística, elas podem influenciar ou contribuir com mais de um objetivo estratégico. Essa relação foi mostrada através das setas de ligação.

Por exemplo, a iniciativa IE3, que objetiva fomentar a indústria doméstica de circuitos integrados, é uma ação que está diretamente relacionada aos aspectos orçamentários do planejamento governamental (OE-I), além de contribuir, em grande parte, para a pesquisa e a inovação (OE-III).

As demais ligações serão explicadas nos tópicos a seguir.

5.1.1 Iniciativa Estratégica 1: Formalizar parceria com Escolas de Governo para inserção de cursos e/ou disciplinas de SIC e SegCiber.

É necessário que o Brasil institua programas de capacitação de agentes públicos, civis e militares, em temas relacionados à ameaça emergente do hardware Trojan. Conforme ressaltou o Livro Branco de Defesa Nacional [131], a proteção do espaço cibernético abrange um grande número de áreas, incluindo a capacitação e a pesquisa científica.

De fato, observa-se que alguns países já vem estruturando conhecimento na área, tratando o tema de forma institucional em suas estruturas governamentais, ou por meio da atuação de universidades [31].

Um exemplo é a Austrália. Em 2008, o Governo Australiano publicou, no âmbito de seu Departamento de Defesa (*Australian Government Department of Defence*), um estudo conceitual sobre hardware Trojan intitulado *Towards Countering the Rise of the Silicon Trojan* [123]. Em 2011, novo estudo foi publicado pelo mesmo órgão (*Hardware Trojans - Prevention, Detection, Countermeasures*), dessa vez abordando ampla revisão bibliográfica sobre prevenção, detecção e contramedidas [31];

Do ponto de vista acadêmico, constatou-se, nos resultados do enfoque meta-analítico apresentados no Capítulo 2, que Estados Unidos, China, Índia, França, Japão e Alemanha estão entre os países com maior produção de pesquisas sobre o tema. Nas bases pesquisadas, não se verificou nenhum estudo produzido no Brasil sobre o assunto, o que evidencia a necessidade do país investir em pesquisas sobre o tema.

A Tabela 5.2 traz a aplicação da metodologia 5W2H no detalhamento dessa iniciativa estratégica.

A presente iniciativa envolve a formação de parceria com Escolas de Governo. As escolas de governo no Brasil desempenham papel fundamental para o provimento das competências necessárias ao aperfeiçoamento das organizações públicas e constituem a

Tabela 5.2: Detalhamento da Iniciativa Estratégica 1 (IE1), utilizando-se a técnica 5W2H

O que?	Formalizar parceria com Escolas de Governo para inserção de cursos e/ou disciplinas de SIC e SegCiber.
Quando?	2019.
Por que?	Para que se forme conhecimento sobre a temática de HT, no âmbito nacional, de forma a preparar o país no enfrentamento da ameaça.
Onde?	Escola Nacional de Defesa Cibernética (ENaDCiber) e Escola Nacional de Administração Pública (ENAP).
Quem?	Órgão central (GSI/PR), com o assessoramento do CGSI.
Como?	(1) Articular junto à ENaDCiber a implementação de módulos introdutório, intermediário e avançado sobre hardware Trojan em cursos de SIC e SegCiber ministrados pela instituição; (2) Articular junto à ENAP a implementação de módulos introdutório, intermediário e avançado sobre hardware Trojan em cursos de SIC e SegCiber ministrados pela instituição
Quanto?	Valor limitado ao orçamento previsto no Programa nº 2058 (Defesa Nacional) do Plano Plurianual 2016-2019, Anexo I [132].

infraestrutura especializada para o desenvolvimento de quadros de servidores, gestores e agentes públicos que formulam e implementam políticas públicas [133].

As duas escolas propostas para uma parceria inicial foram as federais ENAP e ENaDCiber. A Escola Nacional de Administração Pública (ENAP) é uma Escola de Governo do Poder Executivo Federal que oferece formação e aperfeiçoamento em Administração Pública a servidores públicos federais. É vinculada ao Ministério do Planejamento, Desenvolvimento e Gestão e foi criada em 1986. A missão do órgão, conforme declarada em seu Planejamento Estratégico 2016-2019 [134], é o desenvolvimento de competências de servidores públicos para aumentar a capacidade de governo na gestão das políticas públicas.

Portanto, a ENAP foi escolhida no âmbito da presente iniciativa estratégica por sua atuação de excelência na formação de servidores federais, em particular no escopo de formação de gestores em políticas públicas. Conforme ressaltou Alves [135], a ENAP se destaca como uma das principais escolas de governo no Brasil, sendo notável seu trabalho na formação de carreiras de Estado no país.

Por outro lado, a Escola Nacional de Defesa Cibernética (ENaDCiber), conforme descrita no Capítulo 4, foi criada recentemente na estrutura do Exército Brasileiro. Tem como objetivo criar uma "célula nacional", capaz de absorver e disseminar as capacitações relativas à defesa cibernética, reduzindo as lacunas nas áreas de pesquisa, desenvolvimento, operação e gestão da Defesa Cibernética nos níveis de sensibilização, conscientização, formação e especialização [136]. Sua escolha no âmbito dessa iniciativa se deve ao fato de

ser a primeira escola de governo exclusivamente dedicada à temática cibernética.

O ano de 2019 foi definido por ser o primeiro ano de vigência da futura nova versão da Estratégia de SIC e SegCiber. Além disso, trata-se de prazo razoável para que se firme parceria inicial com as duas escolas citadas.

No contexto da iniciativa, propõe-se que os valores tenham como referência o orçamento previsto no Programa nº 2058 (Defesa Nacional) do PPA 2016-2019.

O PPA 2016-2019 é instrumento de planejamento governamental que define diretrizes, objetivos e metas da administração pública federal para as despesas de capital e outras delas decorrentes e para as relativas aos programas de duração continuada, com o propósito de viabilizar a implementação e a gestão das políticas públicas [132]. É papel do Plano, além de declarar as escolhas do governo e da sociedade, indicar os meios para a implementação das políticas públicas, bem como orientar taticamente a ação do Estado para a consecução dos objetivos pretendidos [137].

Os chamados Programas Temáticos compõem essa dimensão tática do PPA. Retratam as agendas de governo, organizadas por recortes selecionados de Políticas Públicas que orienta a ação governamental [137].

O Programa Temático nº 2058 - Defesa Nacional - abarca grande parte das iniciativas da área cibernética no PPA, inclusive a criação do Comando de Defesa Cibernética (iniciativa 05OO) e da própria Escola Nacional de Defesa Cibernética (iniciativa 05OP) [132].

Conforme estrutura da Figura 5.1, a IE1 envolve ações diretamente relacionadas com o Objetivo Estratégico III (OE-III) da Estratégia de SIC e SegCiber, que busca garantir continuamente a pesquisa, o desenvolvimento e a inovação em SIC e SegCiber na APF. Além disso, traz contribuições para o OE-II (garantir continuamente o aprimoramento do quadro de pessoal da APF em SIC e SegCiber, de forma qualitativa e quantitativa), uma vez que pode envolver a qualificação de servidores federais, civis e militares, no âmbito das instituições de ensino; e para o OE-VI (ampliar e fortalecer ações colaborativas em SIC e SegCiber com a academia, setores público, privado e terceiro setor, no país e no exterior), dado que envolve a criação de parcerias com o setor acadêmico.

5.1.2 Iniciativa Estratégica 2: Estabelecer respaldo normativo e jurídico para auditoria de hardware adquirido pelo Governo

É fundamental estruturar respostas normativas, legais ao problema. Conforme mencionado nesse estudo, a legislação vigente ainda é focada no software como ponto de falha na segurança da informação, não havendo referências, ao menos de forma direta, à questão do hardware Trojan.

Conforme visto no Capítulo 4, o Decreto nº 8.135/2013 [11] dispôs que os programas e equipamentos destinados às atividades de comunicação de dados na administração pública federal deverão ter características que permitam auditoria para fins de garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações. No entanto, o decreto não abordou detalhes dessa auditoria, deixando a tarefa para a legislação infralegal.

Os termos do Decreto nº 8.135/2013 foram complementados pela Portaria nº 141 [121]. O dispositivo regulamentar prevê, no seu art. 13, que a auditoria deve ser conduzida pelo órgão ou entidade contratante ou por instituição credenciada pelo governo federal para tal finalidade.

Ainda segundo o regulamento, o governo deverá exigir, no mínimo, a possibilidade de abertura do código fonte no caso de programas para comunicação de dados; e de *firmware* e sistemas operacionais, no caso de equipamentos para comunicação de dados.

Observa-se que não há previsão expressa de auditoria em hardware, que permita a verificação direta de circuitos integrados.

A Tabela 5.3 traz a aplicação da metodologia 5W2H no detalhamento dessa iniciativa estratégica.

Tabela 5.3: Detalhamento da Iniciativa Estratégica 2 (IE2), utilizando-se a técnica 5W2H

O que?	Estabelecer respaldo normativo/jurídico para auditoria de hardware adquirido pelo Governo.
Quando?	2020.
Por que?	Para que o país possa exigir e se utilizar de mecanismos de auditoria em equipamentos de tecnologia da informação e comunicações, adquiridos pelo governo.
Onde?	No âmbito do Executivo Federal
Quem?	Órgão central (GSI/PR), com o assessoramento do CGSI e participação do Ministério do Planejamento, Desenvolvimento e Gestão (MP), Ministério da Defesa (MD) e Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC).
Como?	Promover ajustes na Portaria Interministerial nº 141, de 2 de maio de 2014, de forma a prever a possibilidade de auditoria em hardware e em circuitos integrados.
Quanto?	Por envolver iniciativas legislativas, não há consumo de recursos de forma direta.

Os ajustes promovidos na Portaria devem permitir auditoria no hardware, incluindo os circuitos integrados.

Sugere-se prazo até 2020 para a conclusão da iniciativa, abarcando, portanto, metade da vigência da futura Estratégia de SIC e SegCiber, caso ela venha a ser lançada nos

moldes atuais, com vigência de quatro anos (2019-2022). Ou seja, um prazo de dois anos, compatível com a média de tramitação de projetos legislativos iniciadas pelo Poder Executivo, que gira em torno de 906 dias [138].

A participação do Ministério da Planejamento, Desenvolvimento e Gestão (MP), Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) e Ministério da Defesa se justifica por terem sido os signatários da Portaria Interministerial nº 141/2014.

Conforme estrutura da Figura 5.1, a IE2 envolve ações diretamente relacionadas com o Objetivo Estratégico VII (OE-VII) da Estratégia de SIC e SegCiber, ou seja, a possibilidade de auditar os equipamentos adquiridos pelo Governo Central contribui para elevar o nível de maturidade de SIC e de SegCiber na APF.

5.1.3 Iniciativa Estratégica 3: Fomentar a indústria doméstica de circuitos integrados

A iniciativa diz respeito à indústria de semicondutores. Evidenciou-se, ao longo da pesquisa, que a implementação de códigos maliciosos no nível do hardware é um problema ligado, em essência, à aquisição de equipamentos de tecnologia da informação e comunicações.

Se fosse possível ao Estado produzir todos os seus equipamentos, incluindo os circuitos integrados que os compõem, certamente haveria maior controle sobre o processo, e os riscos seriam menores. No entanto, considerando toda a complexidade envolvida na fabricação de circuitos integrados e a necessidade econômica da globalização da cadeia de suprimentos, tornou-se inviável o domínio de todas as fases da produção.

No contexto do Brasil, país altamente dependente da tecnologia importada de países industrializados, os incentivos à indústria doméstica de circuitos integrados representam parte de uma solução de longo prazo, com extensa margem para aprimoramentos. Conforme bem pontuou Filippin [16], a história tem mostrado que o apoio governamental é fundamental para o sucesso desse setor.

Então é necessário que haja no país um projeto consistente e contínuo de fortalecimento de sua indústria de semicondutores, como forma de construir, ao longo dos anos, o conhecimento necessário para lidar com os desafios da segurança cibernética e, paralelamente, reduzir sua dependência em relação a outros países.

A Tabela 5.4 traz a aplicação da metodologia 5W2H no detalhamento dessa iniciativa estratégica.

Sugere-se prazo até 2023 de forma a coincidir com todo o período do próximo PPA, previsto para o quadriênio 2020-2023.

Tabela 5.4: Detalhamento da Iniciativa Estratégica 3 (IE3), utilizando-se a técnica 5W2H

O que?	Fomentar a indústria doméstica de circuitos integrados.
Quando?	até 2023.
Por que?	Para construir, ao longo dos anos, o conhecimento necessário para lidar com os desafios da segurança cibernética e, paralelamente, reduzir a dependência tecnológica em relação a outros países.
Onde?	No âmbito do Executivo Federal
Quem?	Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) e Ministério da Indústria, Comércio Exterior e Serviços (MDIC).
Como?	(1) Inserção de metas e iniciativas de incentivo específico à indústria de semicondutores, no âmbito do Programa nº 2021 (Ciência, Tecnologia e Inovação) do PPA 2016-2019 [132], estendendo-as para o PPA 2020-2023; (2) Aperfeiçoamento e ampliação do alcance do Programa de Apoio ao Desenvolvimento Tecnológico da Indústria de Semicondutores (PADIS), revendo a legislação atual.
Quanto?	Valor inicialmente limitado ao orçamento previsto no Programa nº 2021 (Ciência, Tecnologia e Inovação) do PPA 2016-2019, Anexo I [132].

Propõe-se a inserção de metas e iniciativas de incentivo específico à indústria de semicondutores, no âmbito do Programa nº 2021 (Ciência, Tecnologia e Inovação) do PPA. O programa foi escolhido pela coerência com a iniciativa proposta, uma vez que já aborda objetivos afins, a exemplo do Objetivo 0486 (Promover a pesquisa, o desenvolvimento e a inovação em tecnologias digitais, componentes e dispositivos eletrônicos), Objetivo 0497 (Promover a formação, capacitação e fixação de recursos humanos qualificados voltados à ciência, tecnologia e inovação), Objetivo 1056 (Promover o desenvolvimento tecnológico e a inovação nas empresas e nas cadeias produtivas) e Objetivo 1057 (Promover políticas e programas de pesquisa, desenvolvimento e inovação e disseminar dados e informações em áreas estratégicas) [132].

Propõe-se, ainda, o aperfeiçoamento e ampliação do PADIS. Conforme foi visto no Capítulo 1, o Programa de Apoio ao Desenvolvimento Tecnológico da Indústria de Semicondutores (PADIS) foi instituído no âmbito da Lei nº 11.484, de 31 de maio de 2007 [139] e dispõe, dentre outros, de incentivos às indústrias de componentes eletrônicos semicondutores e sobre a proteção à propriedade intelectual de circuitos integrados.

Por fim, propõe-se que os valores tenham como referência o orçamento previsto no Programa nº 2021 (Ciência, Tecnologia e Inovação) do PPA, por sua afinidade com a iniciativa, conforme explanado acima.

Conforme estrutura da Figura 5.1, a IE3 envolve ações diretamente relacionadas com o Objetivo Estratégico I (OE-I) da Estratégia de SIC e SegCiber, ou seja, o desenvolvimento da indústria nacional de semicondutores envolve alocações orçamentárias do Governo Cen-

tral; e também o Objetivo Estratégico III (OE-III), uma vez que a inovação, a pesquisa e o desenvolvimento devem ser garantidos para o avanço da indústria de circuitos integrados.

5.1.4 Iniciativa Estratégica 4: Estabelecer, em nível nacional, capacidade de coordenação de respostas rápidas a um ataque de HT

A Estratégia de SIC e SegCiber [12] declarou, como princípio norteador, a importância de se contribuir com a criação de uma robusta capacidade de posicionamento e de respostas da Nação frente às potenciais quebras de segurança e ameaças cibernéticas, fortalecendo a alocação de recursos financeiros, tecnológicos e humanos.

Declarou ainda a resiliência como outro princípio, de forma a contribuir com o aumento da capacidade de resiliência dos ativos de informação e das infraestruturas críticas.

O enfoque da presente iniciativa recai sobre as estruturas organizacionais. O país precisa fortalecer as áreas do governo que lidam com questões relativas à segurança da informação, inclusive aprimorando a comunicação e a interação dessas áreas.

Dessa forma, todas as instâncias do Estado deverão contribuir para o incremento do nível de Segurança Nacional, com particular ênfase, dentre outros, sobre [104]:

- o aperfeiçoamento de processos para o gerenciamento de crises;
- a integração de todos os órgãos do Sistema de Inteligência Nacional (SISBIN);
- as medidas para a segurança das áreas de infraestruturas críticas, incluindo serviços, em especial no que se refere à energia, transporte, água e telecomunicações, a cargo dos Ministérios da Defesa, das Minas e Energia, dos Transportes, da Integração Nacional e das Comunicações, e ao trabalho de coordenação, avaliação, monitoramento e redução de riscos, desempenhado pelo GSI;
- 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 restabelecimento, a cargo da Casa Civil da Presidência da República, dos Ministérios da Defesa, das Comunicações e da Ciência e Tecnologia, e do GSI;

Conforme observou Villasenor [24], é necessário que se estabeleça uma capacidade em âmbito nacional de coordenação e resposta a possíveis ataques de hardware. Como o Brasil não vem produzindo conhecimento nesta área específica, não está claro como o país reagiria ao um ataque dessa natureza.

Tabela 5.5: Detalhamento da Iniciativa Estratégica 4 (IE4), utilizando-se a técnica 5W2H

O que?	Estabelecer, em nível nacional, capacidade de coordenação de respostas rápidas a um ataque de HT.
Quando?	2022.
Por que?	Para que o país possa somar esforços em eventual enfrentamento a um ataque coordenado de HT, evitando ou minimizando os impactos decorrentes.
Onde?	No âmbito do Executivo Federal
Quem?	Conselho de Defesa Nacional (CDN) e GSI/PR; Casa Civil da Presidência da República; Ministério da Defesa (MD), com participação do Comando de Defesa Cibernética do Exército Brasileiro (ComDCiber); e Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC).
Como?	Incluir abordagem sobre ataques de HT no resultado do Grupo de Trabalho criado, no âmbito da Meta M-XXV da Estratégia de SIC e SegCiber, para a modelagem e o planejamento de exercícios de ataques cibernéticos às redes da APF.
Quanto?	A ação preliminar proposta não envolve custos diretos.

A Tabela 5.5 traz a aplicação da metodologia 5W2H no detalhamento dessa iniciativa estratégica.

Sugere-se prazo até 2022 como forma de se utilizar de todo o período de vigência da próxima Estratégia de SIC e SegCiber, caso ela venha a ser lançada nos moldes atuais, com vigência de quatro anos (2019-2022).

Conforme estrutura da Figura 5.1, a iniciativa IE4, que envolve esforços no sentido do estabelecimento de uma capacidade de coordenação de respostas rápidas a um ataque de hardware Trojan, é um desafio complexo diretamente ligado ao nível de maturidade de SIC e SegCiber do país (OE-VII). Uma vez atingida, essa capacidade certamente contribuiria para o fortalecimento da coordenação e da governança sistêmica de SIC e SegCiber (OE-IV) e reforçaria a SIC e a SegCiber como alta prioridade na agenda de governo (OE-VIII). Além disso, a implementação de capacidade de resposta e resistência a um ataque de HT fortaleceria a segurança das infraestruturas críticas da informação, contribuindo para o objetivo OE-IX da Estratégia de SIC e SegCiber.

5.1.5 Iniciativa Estratégica 5: Criar meios de estabelecer um programa de confiança na fabricação de circuitos integrados

Conforme visto, a preocupação com a confiança dos CIs vem crescendo com a globalização de sua cadeia de suprimentos. Por razões econômicas, a separação entre o design e

a manufatura tornou-se inevitável, e grande parte das indústrias de manufatura estão localizadas fora dos territórios nacionais, principalmente em países asiáticos. Há, portanto, uma perda de controle na cadeia de fabricação de circuitos integrados, hoje globalizada.

O relatório *Discussion Draft of the Preliminary Cybersecurity Framework*, do National Institute of Standards and Technology [140], destacou que o gerenciamento de risco da cadeia de suprimentos, particularmente em termos da integridade de produtos e serviços, é uma disciplina emergente caracterizada por diversas perspectivas, distintas áreas de conhecimento e padrões dispersos. Portanto, lidar com o problema é uma questão complexa, e deve envolver, necessariamente, uma perspectiva de tratamento do risco, dado que a ameaça dificilmente será totalmente eliminada, considerando todas as particularidades presentes no tema.

Se é economicamente inviável que os países detenham o controle do ciclo de produção de todos os circuitos integrados utilizados no governo, uma saída viável seria obter, pelo menos, o controle de circuitos integrados utilizados em aplicações mais críticas, a exemplo dos sistemas de defesa.

Soluções pontuais são possíveis. Em 2007, a agência americana *Defense Advanced Research Projects Agency* (DARPA), o braço de pesquisa do Departamento de Defesa dos Estados Unidos, lançou o programa *Trust in Integrated Circuits* (Confiança em CIs), com o objetivo de assegurar que os chips funcionem conforme projetados, assegurando a confiança do processo de design e fabricação [26] [31] [24] [37]. Em 2011, o programa evoluiu para o Projeto IRIS (*Integrity and Reliability of Integrated Circuits*) [26] [27].

Outra iniciativa em solo americano é conduzida pelo *Trusted Access Program Office* (TAPO), da *National Security Agency* (NSA) - a agência de inteligência de sinais do governo dos Estados Unidos - que procura garantir tecnologias seguras na área de microeletrônica aplicada a sistemas críticos daquele país. Ainda assim, o programa só consegue atender uma pequena fração dos chips utilizados nos sistemas de defesa americanos, conforme pontuou Villasenor [26] [37].

Um projeto europeu, conduzido no âmbito do *European Cooperation in Science and Technology* (COST ou COST Action) e intitulado *Trustworthy Manufacturing and Utilization of Secure Devices*, objetiva a criação de uma rede europeia de competência e expertise em todos os aspectos da segurança do hardware, incluindo design, manufatura, testes, confiabilidade, validação e utilização [27]. A rede de conhecimento exercerá papel importante no desenvolvimento de soluções que equacionem os desafios da segurança de hardware, fortalecendo a posição da Europa na área.

Em 2015, a China também iniciou um projeto no âmbito da Natural Science Foundation of China (NSFC), que objetiva criar contramedidas para os riscos de segurança dos CIs [27].

Tendo em vista os fundamentos apresentados, a presente iniciativa estratégica proposta objetiva a criação de meios para o estabelecimento de um programa de confiança na fabricação de circuitos integrados no Brasil.

A Tabela 5.6 traz a aplicação da metodologia 5W2H no detalhamento dessa iniciativa estratégica.

Tabela 5.6: Detalhamento da Iniciativa Estratégica 5 (IE5), utilizando-se a técnica 5W2H

O que?	Criar meios de estabelecer um programa de confiança na fabricação de circuitos integrados.
Quando?	2022.
Por que?	Para que o país possa ao menos assegurar a confiabilidade dos circuitos integrados utilizados em sistemas altamente críticos, como os sistemas de defesa nacional.
Onde?	No âmbito do Executivo Federal
Quem?	GSI/PR; Ministério da Defesa (MD); Ministério das Relações Exteriores (MRE); Ministério da Indústria, Comércio Exterior e Serviços (MDIC); Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC); Cepesc/ABIN.
Como?	(1) Criação de um Grupo de Trabalho interministerial com vistas a avaliar ações para o estabelecimento de um programa de confiança da fabricação de circuitos integrados utilizados em sistemas críticos, demonstrando os custos envolvidos, os desafios, as particularidades, cronograma estimando, dentre outros; (2) Apresentação de proposta de estabelecimento de parcerias estratégicas com países que possam contribuir para o desenvolvimento do programa de confiança na fabricação de circuitos integrados.
Quanto?	A ação preliminar proposta não envolve custos diretos.

Considerando a complexidade envolvida na iniciativa proposta, sugere-se prazo até 2022 como forma de se utilizar de todo o período de vigência da próxima Estratégia de SIC e SegCiber, caso ela venha a ser lançada nos moldes atuais, com vigência de quatro anos (2019-2022).

Conforme estrutura da Figura 5.1, a iniciativa IE5 contribui diretamente para o OE-VI, uma vez que envolverá ações colaborativas de SIC e SegCiber com outros países. Além disso, a implementação de um programa de confiança na fabricação de circuitos integrados contribuiria para a elevação da maturidade de SIC e SegCiber na APF, ao reduzir os riscos de ataques de HT, contribuindo para o objetivo OE-VII da Estratégia de SIC e SegCiber. A iniciativa traria ainda ganhos para a segurança dos sistemas das infraestruturas críticas da informação, afetando a consecução do OE-IX na Estratégia de SIC e SegCiber.

A Figura 5.2 (criação do autor) representa uma visão esquemática das iniciativas propostas, e suas ligações com órgãos que estão relacionados, direta ou indiretamente,

à área cibernética no Brasil, e ilustra a complexidade do tema. Nota-se que políticas públicas criadas objetivando equacionar os desafios da segurança e defesa cibernética devem envolver diversos órgãos, e ter atuação transversal, integradora, interdisciplinar e multissetorial [12], dado a complexidade inerente à matéria.

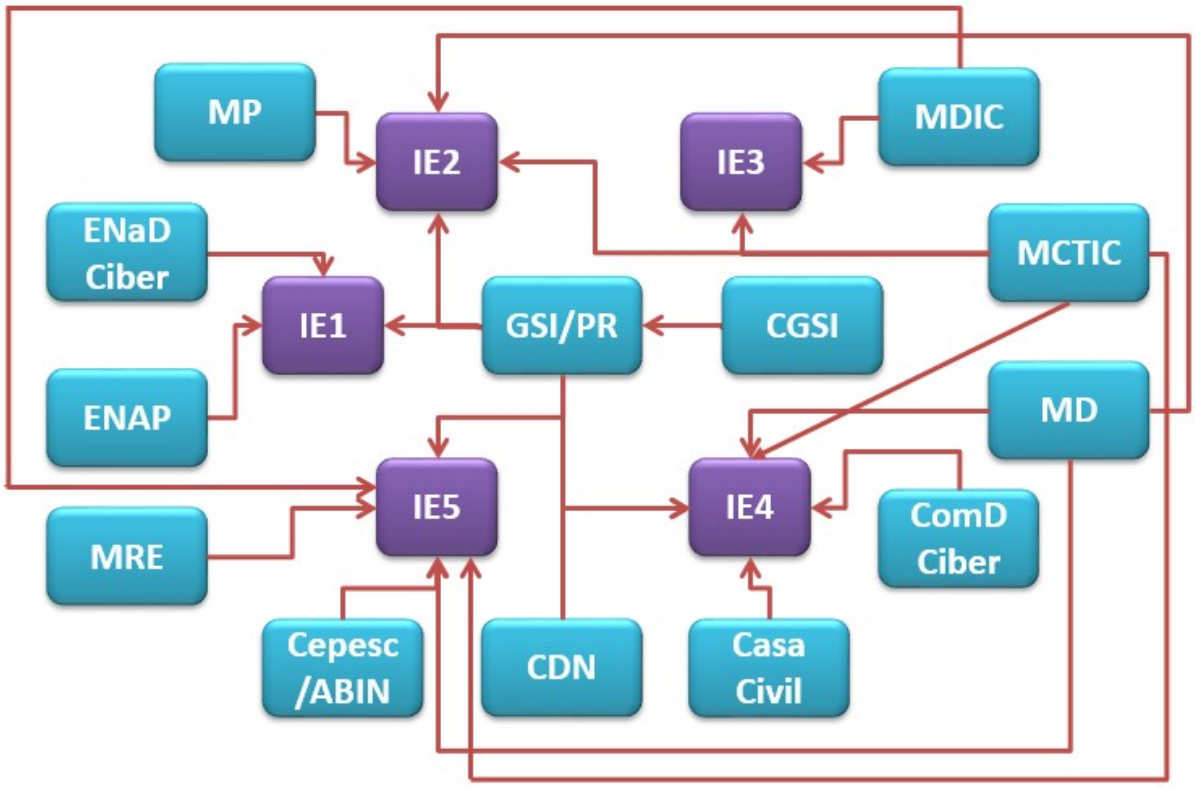

Figura 5.2: Relação entre iniciativas propostas e os órgãos da Administração Pública Federal.

Capítulo 6

Conclusões e Recomendações para Trabalhos Futuros

6.1 Conclusões

O presente trabalho apresentou, em atendimento ao objetivo geral, propostas de desdobramento, no nível tático, dos Objetivos Estratégicos que já estavam declarados na Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018, documento elaborado pelo Poder Executivo Federal e que procurou coordenar esforços e estabelecer diretrizes para o planejamento e o aprimoramento da área de SIC e SegCiber no governo. As propostas permitiram, em linhas gerais, introduzir ações que pudessem chamar a atenção do Governo brasileiro para a ameaça. Espera-se que o debate possa se estender para as diversas instâncias do Governo Federal.

O desdobramento se deu no contexto de uma abordagem específica de segurança cibernética, tratando questões afetas à ameaça do hardware Trojan que, conforme visto, envolve modificações maliciosas no nível do circuito integrado.

Foram propostas 5 iniciativas estratégicas que podem ser contempladas em versões futuras da Estratégia de SIC e SegCiber. As iniciativas incluem ações que se inserem nas 4 perspectivas do BSC declaradas pela Estratégia (Orçamento; Aprendizado, Crescimento e Inovação; Governo; e Resultados para a Sociedade) e abordam aspectos relacionados com capacitação e formação de conhecimento na área; construção de mecanismos jurídicos para o enfrentamento à ameaça; fomento à indústria doméstica de semicondutores; estabelecimento de capacidade de resposta coordenada à ataques de HT; e criação de meios para estabelecimento de programa de confiança na fabricação de circuitos integrados, em particular àqueles utilizados em áreas críticas do Governo.

Constatou-se ainda que as 5 iniciativas estratégicas propostas tem influência direta ou indireta em ao menos 8 dos 10 objetivos estratégicos propostos na Estratégia de SIC e SegCiber.

Verificou-se ainda que as propostas podem contribuir diretamente com duas das metas da própria Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018: a Meta M-XXX, a ser atingida em 2018, que objetiva "levantar novos elementos estratégicos e elaborar a Estratégia de SIC e SegCiber da APF 2019-2022"; e a meta M-XXXVII, a ser atingida no quadriênio 2015-2018, que objetiva "avaliar e revisar a Estratégia de SIC e SegCiber da APF 2015-2018" [12].

O presente estudo também constatou que, não obstante os avanços obtidos por meio de políticas públicas nos últimos anos, a indústria brasileira de circuitos integrados permanece incipiente, fazendo do Brasil uma nação dependente da importação de tecnologia dos países industrializados.

Constatou-se que há uma lacuna nesse desenvolvimento, sendo necessária a ampliação dos esforços no aprimoramento do setor no Brasil, em particular a partir da ação do próprio governo.

A ausência de dispositivos legais que permitam uma auditoria no hardware adquirido por meio de licitações governamentais também é um entrave às ações de prevenção do Estado.

Dessa forma, observa-se que o Estado brasileiro se encontra vulnerável à ameaça do hardware Trojan, não só pela incapacidade de detecção da ameaça nos equipamentos adquiridos, mas pela ausência, por parte do Governo, de ações coordenadas que possam traçar caminhos possíveis para o gerenciamento do problema. Esse, portanto, foi o grande objetivo dessa pesquisa, ou seja, a proposição de ações iniciais, preliminares, mas possíveis de serem tomadas no médio e longo prazo, como forma de fazer com que o País avance no tratamento da ameaça do hardware Trojan.

As ações, no entanto, devem fazer parte de políticas públicas pensadas em abordagem transversal e multissetorial [12]. Observou-se que vários seriam os órgãos e entidades envolvidas em um esforço contínuo e coordenado para lidar com a ameaça do HT, os quais se destacam: Casa Civil; Gabinete de Segurança Institucional; Agência Brasileira de Inteligência; Ministério do Planejamento, Desenvolvimento e Gestão; Conselho de Defesa Nacional; Ministério da Defesa; Comando de Defesa Cibernética; Escola Nacional de Administração Pública; Escola Nacional de Defesa Cibernética; Ministério da Ciência, Tecnologia e Inovações e Comunicações; Ministério da Indústria, Comércio Exterior e Serviços; Ministério das Relações Exteriores; dentre outros.

Dentre os objetivos específicos, na pesquisa sobre a ameaça do hardware Trojan,

observou-se, por meio dos estudos, que o potencial lesivo do hardware Trojan é preocupante, com ações que incluem vazamento de dados, ataques de indisponibilidade, disrupção de sistemas, dentre outros.

Observou-se que o fenômeno envolve uma quebra importante de paradigma na área cibernética, dado que comumente as ameaças são baseadas em software, e não em hardware, em que geralmente a confiabilidade é uma premissa.

O levantamento bibliográfico sobre o tema hardware Trojan foi realizado por meio do enfoque meta-analítico, no qual se contatou que o tema vem ganhando destaque na pesquisa mundial, em particular nos últimos 5 anos.

Com relação às implicações do hardware Trojan no contexto da segurança da informação e da segurança cibernética, constatou-se que o fenômeno hardware Trojan vem preocupando os governos de diversos países, notadamente por envolver, no contexto da guerra cibernética, delicadas questões de espionagem e soberania. De forma geral, países vem tentando lidar com a ameaça e mitigar os riscos associados, uma vez que o problema não pode ser totalmente eliminado.

Observou-se que o fenômeno traz importantes implicações no contexto da segurança da informação e da segurança cibernética. A perda de controle na cadeia de suprimento de circuitos integrados, consequência de um modelo forçosamente globalizado por questões de viabilidade econômica, aliada ao crescimento do complexidade dos chips, trouxeram relevantes desafios não só para a prevenção da ameaça, como para a sua detecção.

Como a grande maioria dos sistemas críticos de um país é baseada em arquiteturas que utilizam a inteligência de circuitos integrados, a ameaça pode trazer relevantes prejuízos para a segurança nacional.

Analisando as implicações do fenômeno hardware Trojan em questões relativas à segurança cibernética brasileira, constatou-se que, no Brasil, pouco se tem falado sobre o tema, não obstante as diversas pesquisas já estabelecidas no meio acadêmico mundial, conforme se identificou por meio do levantamento bibliográfico.

É razoável supor que um governo que empreende grandes aquisições de equipamentos por meio de licitações públicas seja um alvo potencial de ataques de hardware Trojan. Não obstante, constatou-se que, embora as preocupações com a segurança cibernética tenham evoluído no País a partir de revelações feitas por Edward Snowden sobre supostas ações de espionagem dos EUA no Brasil, as ações do governo ainda permanecem focadas nas comunicações e no software como pontos de falha da segurança cibernética.

Não há referências de forma direta às questões envolvendo o hardware Trojan, e a ausência de dispositivos legais que permitam uma auditoria no hardware adquirido por meio de licitações governamentais fazem do país um alvo provável de ataques implementados por meio de hardware Trojan.

6.2 Recomendações para Trabalhos Futuros

O presente trabalho desenvolveu-se sobre determinadas limitações, conforme exposto no Capítulo 1. Não obstante, acredita-se que os estudos aqui iniciados possam ser ampliados.

Assim, sugere-se, por exemplo, que futuras pesquisas possam ampliar o envolvimento de órgãos de inteligência do Governo e das Forças Armadas, de forma a acrescentar dados qualitativos à pesquisa.

Sugere-se ainda a propositura de um índice de maturidade no enfrentamento do hardware Trojan, para que o país possa acompanhar e medir seus esforços no enfrentamento da ameaça.

Outras sugestões incluem: proposição de novas taxonomias para o hardware Trojan; ampliação do escopo do enfoque meta-analítico no levantamento bibliográfico; estudos sobre como o governo brasileiro pode se beneficiar do uso da tecnologia de *blockchain* para evitar a entrada no país de circuitos integrados falsificados.

Referências

[1] Brasil: *Livro Verde - Segurança Cibernética no Brasil*. Presidência da República, 2010. 1, 2, 53, 54

[2] Dykstra, Josiah: *Essential Cybersecurity Science: Build, Test, and Evaluate Secure Systems*. O'Reilly Media, 2015. 1

[3] Harkins, Malcolm W.: *Managing Risk and Information Security: Protect to Enable*. Apress, 2016, ISBN 1484214560. 1

[4] Cert.BR: *Cartilha de Segurança para Internet - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil*. `https://cartilha.cert.br`, 2017. Acesso: 2017-10-01. 1, 37, 64

[5] Maras, Marie Helen: *Transnational Security*. CRC Press, 2014. 1

[6] Guardian, The: *PlayStation Network hackers access data of 77 million users*. `https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data`, 2011. Acesso: 2017-10-22. 1

[7] News, BBC: *How France's TV5 was almost destroyed by 'Russian hackers'*. `http://www.bbc.com/news/technology-37590375`, 2016. Acesso: 2017-10-22. 1

[8] Symantec: *Symantec Security Center*. `https://www.symantec.com/security_response/writeup.jsp?docid=2017-051310-3522-99`, 2017. Acesso: 2017-10-22. 2

[9] World Economic Forum: *The Global Risks Report 2017 12th Edition*. Relatório Técnico, 2017, ISBN 080116. 2

[10] Brasil: *Decreto nº 8.793, de 29 de junho de 2016. Fixa a Política Nacional de Inteligência*, 2016. 2, 55, 62

[11] Brasil: *Decreto nº 8.135, de 04 de novembro de 2013 - dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional*, 2013. 3, 65, 78

[12] Brasil: *Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018*, 2015. 3, 41, 55, 64, 67, 68, 69, 70, 81, 85, 87

[13] Villard, Aurélie, Alan Lelah e Daniel Brissaud: *Drawing a chip environmental profile: Environmental indicators for the semiconductor industry.* Journal of Cleaner Production, 86:98–109, 2015, ISSN 09596526. 3

[14] Chia-Han Tsaia, Hung-Yi Wua, I-Shuo Chen, Jui-Kuei Chenc e Rih-Wei Yed: *Exploring benchmark corporations in the semiconductor industry based on efficiency.* Journal of High Technology Management Research, páginas 1–20, 2017. 3

[15] Union, The International Telecommunication: *Internet of Things.* `https://link-springer-com.ez54.periodicos.capes.gov.br/article/10.1007/s12599-015-0383-3#CR5`, 2015. Acesso: 2017-11-20. 3

[16] Filippin, Flávia: *Estado e Desenvolvimento: a indústria de semicondutores no Brasil.* Tese de Mestrado, UNICAMP, Campinas, Brasil, 2016. 3, 4, 6, 25, 79

[17] Brasil: *Relatório de Incentivos do Programa PADIS no Triênio 2013/2015.* `http://abisemi.org.br/abisemi/arquivosUpload/EA8FFACE2AE36D12.pdf`, 2017. Acesso: 2017-11-03. 4, 5, 6

[18] SIA: *Semiconductor Industry Association - Global Sales Report.* `https://www.semiconductors.org`, 2017. Acesso: 2017-11-20. 4

[19] Indústria, Comércio Exterior e Serviços Ministério da: *Programa de Apoio ao Desenvolvimento Tecnológico da Indústria de Semicondutores e Displays (PADIS).* http://www.mdic.gov.br/index.php/competitividade-industrial/principais-acoes-de-desenvolvimento-industrial/padis/padis. 4

[20] Becker, Georg T., F. Regazzoni, C. Paar e Wayne P. Burleson: *Stealthy dopant-level hardware trojans.* Cryptographic hardware and embedded systems, CHES 2013, páginas 197–214, 2013. 6, 7, 19, 26, 29, 31, 32, 36, 72

[21] Bhunia, S., Michael S. Hsiao, M. Banga e S. Narasimhan: *Hardware trojan attacks:threat analysis and countermeasures.* Em *Proceedings of the IEEE*, volume 102, páginas 197–214, 2014. 6, 26, 28, 30, 66

[22] Xiao, K, D Forte, Y Jin, R Karri, S Bhunia e M Tehranipoor: *Hardware Trojans: lessons learned after one decade of research.* ACM Transactions on Design Automation of Electronic Systems, 22(1):1–23, 2016. 6, 7, 37

[23] Krieg, Christian, Adrian Dabrowski, Heidelinde Hobel, Katharina Krombholz e Edgar Weippl: *Hardware Malware (Synthesis Lectures on Information Security, Privacy, and Tru).* Morgan & Claypool Publishers, 2013, ISBN 1627052518. 6, 32, 34, 35, 37

[24] Villasenor, John: *Ensuring Hardware Cybersecurity.* Electrical Engineering, 1(9), 2011. 6, 81, 83

[25] Iqbal, Asif: *Understanding Integrated Circuit Security Threats.* `https://sdm.mit.edu/news/news_articles/webinar_021014/iqbal_021014.pdf`, 2011. Acesso: 2017-09-09. 6

[26] Villasenor, J: *Compromised by design: Securing the defense electronics supply chain.* Brookings Institute, 2013. 7, 25, 36, 37, 65, 72, 83

[27] Li, He, Qiang Liu e Jiliang Zhang: *A survey of hardware trojan threat and defense.* Integration, the VLSI journal, 2016. 7, 26, 28, 29, 30, 37, 66, 83

[28] King, S. T., J. Tucek, A. Cozzie, C. Grier, W. Jiang e Y. Zhou: *Designing and implementing malicious hardware.* Em *Proceedings of the 1st* USENIX *workshop on large-scale exploits and emergent threats*, 2008. 7, 31, 32, 66

[29] Villasenor, J: *The hacker in your hardware.* Scientific American, 303(2):82–87, 2010. 7

[30] Rawnsley, Adam: *Can Darpa Fix the Cybersecurity 'Problem From Hell?'.* `https://www.wired.com/2011/08/problem-from-hell/`, 2011. Acesso: 2017-11-22. 7

[31] Beaumont, Mark, Bradley Hopkins e Tristan Newby: *Hardware Trojans - Prevention, Detection, Countermeasures (A Literature Review).* Command, Control, Communications and Intelligence Division, Australian government, 2011. 8, 26, 29, 33, 34, 35, 36, 37, 66, 75, 83

[32] Brasil: *Lei nº 9.883, de 7 de dezembro de 1999 - Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências.*, 1999. 9, 60, 61

[33] Mariano, Ari Melo, Rosario Garcia Cruz e Jorge Arenas Gaitán: *Meta análises como instrumento de pesquisa - uma revisão sistemática da bibliografia aplicada ao estudo das alianças estratégicas internacionais.* Em *Congresso Internacional de Administração - Inovação Colaborativa e Competitividade, 2011. Anais*, 2011. 11, 12, 14, 15, 18, 23, 49

[34] Garcia, C. e C. Ramirez: *El meta análisis como instrumento de investigación en la determinación y análisis del objeto del estudio: Aplicado al estudio de sistema de información.* Em *Congresso de Alicante*, páginas 1–13, 2004. 11, 49

[35] Aghaei Chadegani, Arezoo, Hadi Salehi, Melor M. Md Yunus, Hadi Farhadi, Masood Fooladi, Maryam Farhadi e Nader Ale Ebrahim: *A comparison between two main academic literature collections: Web of science and scopus databases.* Asian Social Science, 9(5):18–26, 2013, ISSN 19112017. 11

[36] Calazans, A. T., R. A. Paldes e E. T. Masson: *Uma revisão sistemática da bibliografia sobre usabilidade móvel utilizando o enfoque meta-analítico.* Espacios, 37(10):18, 2016. 18

[37] Goertzel, K. M.: *Integrated circuit security threats and hardware assurance countermeasures.* The Journal of Defense Software Engineering, páginas 33–38, 2013. 23, 25, 83

[38] *Integrated circuit (IC). Britannica Academic, Encyclopædia Britannica, 12 May. 2016.* `academic-eb-britannica.ez54.periodicos.capes.gov.br/levels/collegiate/article/integrated-circuit/106026`. Acesso: 2017-07-01. 24

[39] Floyd, Thomas L.: *Digital Fundamentals*. Pearson, 2014, ISBN 978-0132737968. 24

[40] Jones, Scotten W.: *Introduction to Integrated Circuit Technology*. IC Knowledge LLC, 2012. 24

[41] Rajendran, J., E. Gavas, J. Jimenez, V. Padman e R. Karri: *Towards a comprehensive and systematic classification of hardware trojans*. Em *Proceedings of 2010 IEEE International Symposium*, páginas 1871–1874, New York, USA, 2010. 26, 28, 29

[42] Tehranipoor, Mohammad e Farinaz Koushanfar: *A survey of hardware trojan taxonomy and detection*. IEEE Design and Test of Computers, 27(1):10–25, 2010, ISSN 07407475. 26, 27, 28, 29, 33, 34, 35, 36, 66

[43] Swierczynski, Pawel, Marc Fyrbiak, Philipp Koppe e Christof Paar: *FPGA Trojans Through Detecting and Weakening of Cryptographic Primitives*. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2015, ISSN 02780070. 26

[44] Baumgarten, Alex, Michael Steffen, Matthew Clausman e Joseph Zambreno: *A case study in hardware Trojan design and implementation*. International Journal of Information Security, 10(1):1–14, 2011, ISSN 16155262. 26, 29, 66

[45] Agrawal, Dakshi, Selcuk Baktir, Deniz Karakoyunlu, Pankaj Rohatgi e Berk Sunar: *Trojan detection using IC fingerprinting*. Proceedings - IEEE Symposium on Security and Privacy, páginas 296–310, 2007, ISSN 10816011. 26, 29, 37, 66

[46] Karri, Ramesh, Jeyavijayan Rajendran e Kurt Rosenfeld: *Trustworthy hardware: Identifying and Classifying hardware Trojans*. IEEE Computer Society, páginas 39–46, 2010. 26, 29, 66

[47] Chakraborty, R. S., S. Narasimhan e S. Bhunia: *Hardware trojan: Threats and emerging solutions*. IEEE, 2009. 26, 28, 29, 30, 34, 35

[48] Clarke, Richard A. e Robert K. Knake: *Guerra Cibernética. A Próxima Ameaça à Segurança e o que Fazer a Respeito*. Brasport, 2015, ISBN 8574527114. 26, 37

[49] Wang, Xiaoxiao, Mohammad Tehranipoor e Jim Plusquellic: *Detecting malicious inclusions in secure hardware: Challenges and solutions*. 2008 IEEE International Workshop on Hardware-Oriented Security and Trust, HOST, 1(July):15–19, 2008. 26, 27, 28, 33, 72

[50] Wolff, Francis, Chris Papachristou, Swarup Bhunia e Rajat S. Chakraborty: *Towards trojan-free trusted ICs: Problem analysis and detection scheme*. Em *Proceedings - Design, Automation and Test in Europe, DATE*, 2008, ISBN 9783981080. 28

[51] Qamarina, Nur, Mohd Noor, Nilam Nur, Amir Sjarif, Nurul Huda, Firdaus Mohd e Salwani Mohd Daud: *Hardware Trojan Identification Using Machine Learning-based Classification*. Journal of Telecommunication, Electronic and Computer Engineering result., 9(3):23–27, 2017. 28, 37, 66

[52] Bhunia, Swarup, Miron Abramovici, Dakshi Agrawal, Michael S. Hsiao, Jim Plusquellic, Mohammad Tehranipoor e Paul Bradley: *Protection against hardware trojan attacks: Towards a comprehensive solution*. IEEE Design and Test, 30(3):6–17, 2013, ISSN 21682356. 28, 66

[53] Salmani, H: *New design strategy for improving hardware trojan detection and reducing trojan activation time*. Hardware-Oriented Security and Trust, 2009. HOST '09. IEEE International Workshop on, páginas 66–73, 2009. 28

[54] Tehranipoor, Mohammad, Hassan Salmani, Xuehui Zhang, Michel Wang, Ramesh Karri, Jeyavijayan Rajendran e Kurt Rosenfeld: *Trustworthy Hardware: Trojan Detection and Design-for-Trust Challenges*. IEE Computer Society, 44(7):66–74, jul 2011, ISSN 0018-9162. 28

[55] Surendar A, Sharma S, Tejaswi V e Ramyasri G: *Surveillance of integrated circuit for Hardware Trojan and remedies to protect from the Trojan*. RJPBCS, 8:317 – 326, 2017, ISSN 0975-8585. 28, 35

[56] Salmani, Hassan, Mohammad Tehranipoor e Jim Plusquellic: *A novel technique for improving hardware trojan detection and reducing trojan activation time*. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 20(1):112–125, 2012, ISSN 10638210. 28

[57] Kelly, Shane, Xuehui Zhang, Mohammed Tehranipoor e Andrew Ferraiuolo: *Detecting Hardware Trojans using On-chip Sensors in an ASIC Design*. Journal of Electronic Testing: Theory and Applications (JETTA), 31(1):11–26, 2015, ISSN 15730727. 28

[58] Malekpour, Amin, Roshan Ragel, Aleksandar Ignjatovic e Sri Parameswaran: *TrojanGuard: simple and effective hardware Trojan mitigation techniques for pipelined MPSoCs*. Em *Proceedings of the 54th Annual Design Automation Conference 2017 on - DAC '17*, páginas 1–6, 2017, ISBN 9781450349277. `http://dl.acm.org/citation.cfm?doid=3061639.3062336`. 28

[59] Shiyanovskii, Y, F Wolff, C Papachristou, D Weyer e W Clay: *Exploiting Semiconductor Properties for Hardware Trojans*. ACM CoRR, página 6, 2009. 32, 66

[60] Chakraborty, R. S., I. Sasha, A. Palchaudhuri e G. K. Naik: *Hardware trojan insertion by direct modification of fpga configuration bitstream*. IEEE Design and Test, 30(2), 2013. 32

[61] Subramani, Kiruba Sankaran, Angelos Antonopoulos, Ahmed Attia Abotabl, Aria Nosratinia e Yiorgos Makris: *INFECT: INconspicuous FEC-based Trojan: A hardware attack on an 802.11a/g wireless network*. Em *Proceedings of the 2017 IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2017*, páginas 90–94, 2017, ISBN 9781538639283. 32, 66

[62] Pikma, T.: *Stealthy dopant-level hardware trojans*. Em *Research Seminar in Cryptography*, 2013. 32, 33

[63] Abramovici, Miron e Paul Bradley: *Integrated circuit security: new threats and solutions*. Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies (CSIIRW 09), páginas 0–2, 2009. http://dl.acm.org/citation.cfm?id=1558671. 33, 35

[64] Bhasin, Shivam, Jean Luc Danger, Sylvain Guilley, Xuan Thuy Ngo e Laurent Sauvage: *Hardware trojan horses in cryptographic IP cores*. Proceedings - 10th Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2013, páginas 15–29, 2013. 35

[65] Schwartau, Winn: *Information Warfare: Chaos on the Electronic Superhighway*. Thunder's Mouth Pr, 1994, ISBN 1560250801. 36

[66] USA: *High Performance Microchip Supply*. Relatório Técnico, Department of Defense, Washington DC, 2005. 36

[67] Li, Jie e John Lach: *At-speed delay characterization for IC authentication and Trojan horse detection*. 2008 IEEE International Workshop on Hardware-Oriented Security and Trust, HOST, páginas 8–14, 2008. 36

[68] Skorobogatov, Sergei e Christopher Woods: *Breakthrough silicon scanning discovers backdoor in military chip*. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 7428 LNCS(March):23–40, 2012, ISSN 03029743. 36

[69] Moein, Samer, Thomas Aaron Gulliver, Fayez Gebali e Abdulrahman Alkandari: *A New Characterization of Hardware Trojans*. IEEE Access, 4:2721–2731, 2016, ISSN 21693536. 37

[70] Papke-Shields, Karen E. e Kathleen M. Boyer-Wright: *Strategic planning characteristics applied to project management*. International Journal of Project Management, 35(2):169–179, 2017, ISSN 02637863. 38

[71] Camillus, John C.: *Reconciling logical incrementalism and synoptic formalism—an integrated approach to designing strategic planning processes*. Strategic Management Journal, 3(3):277–283, jul 1982. https://doi.org/10.1002/smj.4250030309. 38

[72] Fredrickson, J. W. e T. R. Mitchell: *Strategic decision processes: Comprehensiveness and performance in an industry with an unstable environment.* Academy of Management Journal, 27(2):399–423, jun 1984. https://doi.org/10.2307/255932. 38

[73] Meissner, Philip: *A process-based perspective on strategic planning: the role of alternative generation and information integration*. Business Research, 7(1):105–124, 2014, ISSN 2198-3402. 38

[74] *Strategic Planning. Britannica Academic, Encyclopædia Britannica, 11 Nov. 2016*. http://academic-eb-britannica.ez54.periodicos.capes.gov.br/levels/collegiate/article/strategic-planning/601044. Acesso: 2017-11-19. 38, 39

[75] Maximiano, A.: *Introdução À Administração*. Atlas, São Paulo, 2006, ISBN 8522445222. 38, 39, 40

[76] Chiavenato, Idalberto: *Administração Geral e Pública*. Campus, São Paulo, 2008, ISBN 9788535231700. 38, 39, 40

[77] Kotler, Philip: *Administração de marketing*. Editora Atlas, São Paulo, 1975. 38

[78] Almeida, Martinho I.: *Manual de Planejamento Estratégico*. Atlas, São Paulo, 2011. 38

[79] Felix, Rozelito, Patrícia do Prado Felix e Rafael Timóteo: *BSC: Adequação para a Gestão Estratégica nas Organizações Públicas*. Revista do Serviço Público, 62 (1): 51(61), 2011. 38, 40, 41, 43, 44

[80] Chiavenato, Idalberto: *Introdução à Teoria Geral da Administração: Uma Visão Abrangente da Moderna Administração das Organizações*. Elsevier, São Paulo, 2003, ISBN 8535213481. 39, 40

[81] Certo, Samuel C. e J. P. Peter: *Administração Estratégica: Planejamento e Implantação da Estratégia*. Prentice-Hall, 2005, ISBN 8576050250. 39, 41

[82] Alday, Hernan E Contreras: *O Planejamento Estratégico dentro do Conceito de Administração Estratégica*. Revista da FAE, 3; n 2:9–16, 2000, ISSN 00205850. 40

[83] Niven, Paul R.: *Balanced Scorecard Step-by-Step: Maximizing Performance and Maintaining Results*. Wiley, 2002, ISBN 0471078727. 41, 42, 43, 70

[84] Institute, BSC: *Balanced Scorecard Institute - BSC Basis*. `http://www.balancedscorecard.org/BSC-Basics/About-the-Balanced-Scorecard`, 2017. Acesso: 2017-09-30. 41, 42, 43, 45, 70

[85] Kaplan, Robert e David Norton: *A Estratégia em Ação: Balanced Scorecard*. Editora Campus, Rio de Janeiro, RJ, 1997. 42, 43

[86] Costa, Leandro: *O Balanced Scorecard E O Processo Estratégico*. Caderno de Pesquisas em Administração, São Paulo, v.10(4):61–73, 2003. 42

[87] Mello, Celso Antônio Bandeira de: *Curso de Direito Administrativo*. Malheiros, 2015. 44

[88] Kaplan, Robert e David Norton: *Using the Balanced Scorecard as a Strategic Management System*. Harvard Business Review, páginas 75–86, 1996. 45

[89] Walter, Fábio e F. J. Kliemann Neto: *Uma Proposta de Metodologia de Elaboração do "BALANCED SCORECARD"*. Em *VII Congresso Brasileiro de Custos*, páginas 1–16, Recife - PE, 2000. 45

[90] Behr, Ariel, Eliane Lourdes da Silva Moro e Lizandra Brasil Estabel: *Gestão da biblioteca escolar: metodologias, enfoques e aplicação de ferramentas de gestão e serviços de biblioteca*. Ciência da Informação, 37(2):32–42, 2008, ISSN 0100-1965. 45

[91] Nakagawa, Marcelo: *Ferramenta: 5W2H Plano de Ação para Empreendedores.* `http://cms-empreenda.s3.amazonaws.com/empreenda/files_static/arquivos/2014/07/01/5W2H.pdf`, 2014. Acesso: 2017-10-28. 45

[92] Vergara, Sylvia C: *Gestão da Qualidade.* Editora FGV, Rio de Janeiro, RJ, 2006. 47, 73

[93] Gil, Antonio Carlos: *Como elaborar projetos de pesquisa.* Editora Atlas, São Paulo, SP, 2002. 48

[94] Lakatos, Eva M. e Marina A. Marconi: *Fundamentos de Metodologia Científica.* Editora Atlas, São Paulo, SP, 2003. 48, 49, 50

[95] Kauark, Fabiana S., Fernanda C. Manhães e Carlos H. Medeiros: *Metodologia da Pesquisa - Um Guia Prático.* Editora Via Litterarum, Itabuna, BA, 2010. 48, 50

[96] Institute, Project Management: *Um Guia Do Conhecimento Em Gerenciamento De Projetos (Guia PMBOK®)–Quinta Edição (BRAZILIAN PORTUGUESE) (PMBOK® Guide) (Portuguese Edition).* Project Management Institute, 2013. 48

[97] Manzo, Abelardo: *Manual para la preparación de monografias: una guía para presentar informes y tesis.* Humanitas, Buenos Aires, 1971. 48

[98] Sanchez, Julio: *Metodología para la Investigación en Marketing y Dirección de Empresas.* Ediciones Pirámide, Madrid, 1999. 49

[99] Brasil: *Lei nº 9.649, de 27 de maio de 1998 - Dispõe sobre a organização da Presidência da República e dos Ministérios, e dá outras providências.*, 1998. 52, 55

[100] Brasil: *Medida Provisória nº 782, de 31 de maio de 2017 - Estabelece a organização básica dos órgãos da Presidência da República e dos Ministérios.*, 2017. 52, 55, 60, 61

[101] 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, remaneja cargos em comissão e funções de confiança e substitui cargos em comissão do Grupo-Direção e Assessoramento Superiores - DAS por Funções Comissionadas do Poder Executivo - FCPE.*, 2017. 52, 55, 56, 64

[102] Brasil: *Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008 - Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.*, 2008. 52, 53, 56, 57, 67

[103] Brasil: *Portaria GSI nº 91, de 26 de julho de 2017. Aprovar o Regimento Interno do Gabinete de Segurança Institucional da Presidência da República, na forma do anexo a esta Portaria*, 2017. 52

[104] Brasil: *Decreto nº 6.703, de 18 de dezembro de 2008 - Aprova a Estratégia Nacional de Defesa*, 2008. 52, 62, 81

[105] Brasil: *Doutrina Militar de Defesa Cibernética MD31-M-07*, 2014. 52, 53, 54

[106] Brasil: *Decreto nº 3.505, de 13 de junho de 2000 - Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal*, 2000. 53, 56, 57

[107] Brasil: *Glossário das Forças Armadas MD35-G-01*, 2007. 55

[108] Brasil: *Constituição da República Federativa do Brasil, de 5 de outubro de 1988*, 1988. 58, 65, 66

[109] Brasil: *Lei nº 8.183, de 11 de abril de 1991 - Dispõe sobre a organização e o funcionamento do Conselho de Defesa Nacional e dá outras providências.*, 1991. 58, 59

[110] Brasil: *Cria a Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo*, 2003. 60

[111] ABIN: *Cronologia de Criação dos Órgãos de Inteligência de Estado no Brasil*. `http://www.abin.gov.br/institucional/historico/`, 2017. Acesso: 2017-11-20. 61

[112] Brasil: *Decreto nº 8.905, de 17 de novembro de 2016 - Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Agência Brasileira de Inteligência, remaneja cargos em comissão e substitui cargos em comissão do Grupo Direção e Assessoramento Superior - DAS por Funções Comissionadas do Poder Executivo - FCPE.*, 2016. 61, 62

[113] Brasil: *Cria o Centro de Defesa Cibernética do Exército e dá outras providências*, 2010. 63

[114] Brasil: *Ativa o Núcleo do Centro de Defesa Cibernética do Exército e dá outras providências.*, 2010. 63

[115] Brasil: *Decreto nº 7.809, de 20 de setembro de 2012 - Altera os Decretos no 5.417, de 13 de abril de 2005, no 5.751, de 12 de abril de 2006, e no 6.834, de 30 de abril de 2009, que aprovam as estruturas regimentais e os quadros demonstrativos dos cargos em comissão e das funções gratificadas dos Comandos da Marinha, do Exército e da Aeronáutica, do Ministério da Defesa.*, 2012. 63

[116] Brasil: *Decreto nº 5.751, de 12 de abril de 2006 - Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Grupo-Direção e Assessoramento Superiores - DAS e das Funções Gratificadas do Comando do Exército do Ministério da Defesa, e dá outras providências.*, 2006. 63

[117] Brasil: *Decreto nº 8.491, de 13 de julho de 2015 - Altera o Anexo I ao Decreto nº 5.751, de 12 de abril de 2006, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Grupo-Direção e Assessoramento Superiores - DAS e das Funções Gratificadas do Comando do Exército do Ministério da Defesa.*, 2015. 63

[118] Brasil: *Dispõe sobre a diretriz de implantação de medidas visando à potencialização da Defesa Cibernética Nacional e dá outras providências*, 2014. 63

[119] Brasil: *Decreto nº 8.913, de 23 de novembro de 2016 - Altera o Decreto nº 5.751, de 12 de abril de 2006, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções Gratificadas do Comando do Exército, do Ministério da Defesa, remaneja cargos em comissão e funções gratificadas e substitui cargos em comissão do Grupo-Direção e Assessoramento Superiores - DAS por Funções Comissionadas do Poder Executivo - FCPE.*, 2016. 63

[120] Brasil: *Relatório Final nº 01 de 2014 – CPI da Espionagem - Senado Federal*, 2014. 65

[121] Brasil: *Portaria Interministerial nº 141, de 2 de maio de 2014. Dispõe que as comunicações de dados da Administração Pública Federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da Administração Pública Federal*, 2014. 65, 78

[122] Brasil: *Painel do Orçamento Federal - Acesso Público - Despesas de TI*. `https://www1.siop.planejamento.gov.br/QvAJAXZfc/opendoc.htm?document=IAS%2FExecucao_Orcamentaria.qvw&host=QVS%40pqlk04&anonymous=true`, 2017. Acesso: 2017-11-19. 65

[123] Anderson, M S e K K Yiu: *Towards Countering the Rise of the Silicon Trojan*, 2008, ISBN DSTO-TR-2220. 66, 75

[124] Wei, Sheng e Miodrag Potkonjak: *The undetectable and unprovable hardware trojan horse*. Proceedings of the 50th Annual Design Automation Conference on - DAC '13, página 1, 2013, ISSN 0738100X. `http://dl.acm.org/citation.cfm?doid=2463209.2488912`. 66

[125] Çakir, Burçin e Sharad Malik: *Hardware Trojan Detection for Gate-level ICs Using Signal Correlation Based Clustering*. Em *Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition*, páginas 471–476, 2015, ISBN 978-3-9815370-4-8. `http://dl.acm.org/citation.cfm?id=2755753.2755860`. 66

[126] Lin, Lang, Markus Kasper, Tim Güneysu, Christof Paar e Wayne Burleson: *Trojan side-channels: Lightweight hardware Trojans through side-channel engineering*. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 5747 LNCS:382–395, 2009, ISSN 03029743. 66

[127] Bloom, Gedare, Bhagirath Narahari e Rahul Simha: *OS support for detecting trojan circuit attacks*. Em *2009 IEEE International Workshop on Hardware-Oriented Security and Trust, HOST 2009*, número 202, páginas 100–103, 2009, ISBN 9781424448043. 66

[128] Brasil: *Tribunal de Contas da União. Acórdão nº 3051/2014, do Plenário*, 2014. 66, 67

[129] Brasil: *Tribunal de Contas da União. Acórdão nº 3117/2014, do Plenário*, 2014. 67

[130] Brasil: *Portaria CDN nº 14, de 11 de maio de 2015. Homologa a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal - 2015/2018, versão 1.0*, 2015. 67

[131] Brasil: *Livro Branco de Defesa Nacional*, 2012. 75

[132] Brasil: *Lei nº 13.249, de 13 de janeiro de 2016. Institui o Plano Plurianual da União para o período de 2016 a 2019*, 2016. 76, 77, 80

[133] Carvalho, Antônio Ivo de, Anísio Soares Vieira, Fátima Bruno, José Inácio Jardim Motta, Margaret Baroni, Maria Cristina Macdowell, Rosângela Salgado e Sérgio da Costa Côrtes: *Escolas de governo e gestão por competências: mesa-redonda de pesquisa-ação*. ENAP, 2009, ISBN 978-85-256-0063-9. 76

[134] ENAP: *Planejamento Estratégico ENAP 2016-2019*. `http://www.enap.gov.br/web/pt-br/planejamento-estrategico`, 2016. Acesso: 2018-01-08. 76

[135] Alves, Alex C.: *As Escolas de Governo na Profissionalização da Burocracia Brasileira*. Revista de Direito da Administração Pública, 2:32–58, 2016. 76

[136] ENaDCiber: *Perguntas Frequentes - Escola Nacional de Defesa Cibernética*. `https://ava-enadciber.eb.mil.br/mod/page/view.php?id=576`, 2016. Acesso: 2018-01-08. 76

[137] Brasil: *Orientações para a Elaboração do Plano Plurianual 2016-2019*, 2015. 77

[138] Carazza, Bruno: *Quem Controla Quem na Elaboração das Leis Brasileiras*. `https://leisenumeros.com.br/2015/03/quem-controla-quem-na-elaboracao-das-leis-brasileiras/`, 2015. Acesso: 2018-01-09. 79

[139] Brasil: *Lei nº 11.484, de 31 de maio de 2007 - Dispõe sobre os incentivos às indústrias de equipamentos para TV Digital e de componentes eletrônicos semicondutores e sobre a proteção à propriedade intelectual das topografias de circuitos integrados, instituindo o Programa de Apoio ao Desenvolvimento Tecnológico da Indústria de Semicondutores – PADIS e o Programa de Apoio ao Desenvolvimento Tecnológico da Indústria de Equipamentos para a TV Digital – PATVD; altera a Lei no 8.666, de 21 de junho de 1993; e revoga o art. 26 da Lei no 11.196, de 21 de novembro de 2005.*, 2007. 80

[140] USA: *Discussion draft of the preliminary cybersecurity framework [report]*, 2013. 83

Anexo I

Metas Declaradas na Estratégia de SIC e SegCiber da APF 2015-2018

M-I: Definir metodologia e mecanismo de autodiagnóstico de SIC e de SegCiber da APF.

M-II: Atingir no mínimo 25% da APF direta com autodiagnóstico de SIC e de SegCiber acompanhados e avaliados pelo órgão central (GSI/PR).

M-III: Articular e estabelecer programa no PPA 2016-2019 que contemple conjuntamente as temáticas de SIC e de SegCiber

M-IV: Articular e formalizar função orçamentária específica em Segurança Institucional, contemplando subfunção SIC e SegCiber, entre outras.

M-V: Criar a Câmara Multissetorial de SIC e de SegCiber da APF no âmbito do Sistema.

M-VI: Formalizar parceria do órgão central do sistema de SIC e de SegCiber da APF (GSI/PR) com a ENAP/MP para inserção de cursos e/ou de disciplinas de SIC e de SegCiber, visando a formação continuada dos agentes públicos nestas áreas.

M-VII: Propor um guia de boas práticas de planejamento de SIC e de SegCiber para os órgãos e entidades da APF, com base na Norma Complementar nº 02/IN01/DSIC/GSIPR, visando seu alinhamento ao planejamento estratégico institucional.

M-VIII: Propor a criação do "Dia Oficial de SIC e de SegCiber do Governo Federal".

M-IX: Estabelecer o Modelo de Governança Sistêmica de SIC e de SegCiber da APF – nível político estratégico.

M-X: Estabelecer mecanismo para mapeamento sistemático dos ativos de informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade que compõem as infraestruturas críticas da informação.

M-XI: Atingir no mínimo 50% da APF direta com autodiagnóstico de SIC e de SegCiber acompanhados e avaliados pelo órgão central (GSI/PR).

M-XII: Atingir no mínimo 5% da APF indireta com autodiagnóstico de SIC e de SegCiber acompanhados e avaliados pelo órgão central (GSI/PR).

M-XIII: Desenvolver indicador de nível de maturidade de SIC e de SegCiber nos órgãos e entidades da APF, como um mecanismo de acompanhamento e avaliação. O desenvolvimento envolverá, dentre outras, as etapas de debate metodológico, estudos e testes e a definição do indicador.

M-XIV: Articular a inserção das áreas de SIC e de SegCiber no Programa Nacional de Gestão Pública e Desburocratização (GesPública), coordenado pelo MP, no item "Informação e Conhecimento".

M-XV Formalizar parceria do órgão central do sistema de SIC e de SegCiber da APF (GSI/PR) com, no mínimo, mais duas Escolas de Governo, para inserção de cursos e/ou de disciplinas de SIC e SegCiber, visando a formação continuada dos agentes públicos nestas áreas.

M-XVI Articular a criação do ecossistema digital (SIC+SegCiber+Empresas+ICTs), em sintonia com o ecossistema de defesa cibernética.

M-XVII Criar a Comissão para estudo de viabilidade da criação de carreira de Estado de SIC e de SegCiber e respectiva estrutura organizacional, em nível estratégico, no Governo Federal.

M-XVIII Criar Grupo de Trabalho objetivando a modelagem e o planejamento de exercícios de ataques cibernéticos às redes da APF.

M-XIX Promover a "Conferência Bianual de SIC e de SegCiber da APF".

M-XX Implementar e aferir o indicador anual de nível de maturidade de SIC e de SegCiber nos órgãos e entidades da APF, como mecanismo de acompanhamento e avaliação.

M-XXI Atingir no mínimo 75% da APF direta com autodiagnóstico de SIC e de SegCiber acompanhados e avaliados pelo órgão central (GSI/PR).

M-XXII Atingir no mínimo 10% da APF indireta com autodiagnóstico de SIC e de SegCiber acompanhados e avaliados pelo órgão central (GSI/PR).

M-XXIII Propor método de identificação de ameaças e geração de alertas das infraestruturas críticas da informação.

M-XXIV Formalizar parceria do órgão central do sistema de SIC e de SegCiber da APF (GSI/PR) com, no mínimo, mais duas Escolas de Governo, para inserção de cursos e/ou de disciplinas de SIC e de SegCiber, visando a formação continuada dos agentes públicos nestas áreas.

M-XXV Encaminhar o resultado do Grupo de Trabalho de modelagem e planejamento de exercícios de ataques cibernéticos às redes da APF ao órgão central (GSI/PR).

M-XXVI Aferir o indicador anual de nível de maturidade de SIC e de SegCiber nos órgãos e entidades da APF.

M-XXVII Atingir 100% da APF direta com autodiagnóstico de SIC e de SegCiber acompanhados e avaliados pelo órgão central (GSI/PR).

M-XXVIII Atingir no mínimo 15% da APF indireta com autodiagnóstico de SIC e de SegCiber acompanhados e avaliados pelo órgão central (GSI/PR).

M-XXIX Formalizar parceria do órgão central do sistema de SIC e de SegCiber da APF (GSI/PR) com, no mínimo, mais duas Escolas de Governo, para inserção de cursos e/ou de disciplinas de SIC e de SegCiber, visando a formação continuada dos agentes públicos nestas áreas.

M-XXX Levantar novos elementos estratégicos e elaborar a "Estratégia de SIC e de SegCiber da APF 2019-2022".

M-XXXI Encaminhar o resultado do estudo de viabilidade de criação da carreira de Estado de SIC e de SegCiber no Governo Federal ao órgão central (GSI/PR).

M-XXXII Promover a "Conferência Bianual de SIC e de SegCiber da APF".

M-XXXIII Promover anualmente, no âmbito da APF, no mínimo 10 oficinas abordando as Normas Complementares à IN GSI/PR nº 01/2008.

M-XXXIV Anualmente, promover e coordenar no mínimo 2 Colóquios Técnicos sobre tratamento e respostas a incidentes em redes computacionais da APF.

M-XXXV Alinhar, de forma contínua, o planejamento de SIC e de SegCiber dos órgãos e entidades da APF aos respectivos Planejamentos Estratégicos.

M-XXXVI Fortalecer e formalizar parcerias do órgão central do sistema de SIC e de SegCiber da APF (GSI/PR) com universidades e instituições de ensino superior para inserção de cursos e/ou de disciplinas de SIC e de SegCiber no nível da graduação e da pós graduação.

M-XXXVII Avaliar e revisar a "Estratégia de SIC e de SegCiber da APF 2015-2018".

M-XXXVIII Promover campanhas de conscientização da sociedade nas áreas de SIC e de SegCiber.