A Guerra Cibernética: exploração, ataque e proteção cibernética no contexto dos sistemas de Comando e Controle (C²)

Mauro Guedes Ferreira Mosqueira Gomes[1],Sandro Silva Cordeiro [2], Wallace Anacleto Pinheiro[3]*

[1] Diretoria de Fabricação, Praça Duque de Caxias, nº 25 - 7º andar - Centro - Rio de Janeiro/RJ - CEP: 20221-260

[2] Academia Militar das Agulhas Negras – AMAN, Rodovia Presidente Dutra, Km 306 – Resende – RJ, CEP: 27534-970

E-mail: sscordeiro@hotmail.com

[2] Centro de Desenvolvimento de Sistemas – CDS, Quartel General do Exército – Bloco G – 2º Piso – Setor Militar Urbano – Brasília – DF, CEP: 70630-901

RESUMO: *Nenhum sistema de computador é totalmente invulnerável a ataques de um hacker talentoso e determinado. A Guerra Cibernética (G Ciber) é uma arma que pode ser empregada remotamente e de forma anônima. Ela pode ser algumas vezes mais destrutiva e com efeitos de mais longo alcance do que ataques realizados em guerras tradicionais. Para se adaptar às exigências dessa nova forma de combate, a concepção de C2, existente até então, teve que passar por consideráveis alterações, deixando de lado a tradicional dependência de modelos hierárquicos para a fusão de informações e tomada de decisão e adotando estruturas de rede com maior flexibilidade, conectividade lateral e colaboração através das fronteiras organizacionais. Dentro desse contexto, para compreender melhor os efeitos de um Ataque Cibernético contra qualquer sistema de C2, este trabalho elicita as ações cibernéticas típicas que podem ser realizadas por atacantes em sistemas de C2. Além disso, propõe um conjunto de contramedidas (proteções cibernéticas) que podem ser tomadas para evitar ou minimizar os impactos causados por essas ações.*

PALAVRAS-CHAVE: *Guerra Cibernética, Comando e Controle, Proteção Cibernética, vulnerabilidades.*

ABSTRACT: *No computer system is completely invulnerable to a talented and determined hacker. The Cyber War is a weapon that can be used remotely and anonymously. It can be sometimes more destructive than traditional wars attacks. To adapt to the new demands of Cyber War, the concept of C2, existing until then, had to undergo considerable changes, leaving aside the traditional dependence of hierarchical models for the fusion of information and decision making, adopting network structures with greater flexibility, lateral connectivity and collaboration across organizational boundaries. Within this context, to better understand the effects of a Cyber Attack against any C2 system, this article discusses the typical cyber actions that can be performed by attackers to C2 systems. It also proposes a set of countermeasures (cyber protections) that can be taken to avoid or minimize the impacts caused by these actions.*

KEYWORDS: *Cyber War, Command and Control, C2, Hacker, Cyber Protection, vulnerabilities.*

1. Introdução

O século XXI trouxe consigo novos desafios. As missões militares da atualidade são bem diferentes das missões tradicionais dos séculos passados. Elas são simultaneamente mais complexas e mais dinâmicas, exigindo capacidades coletivas e esforços de muitas organizações para se ter sucesso [1].

A expansão significativa, nos últimos tempos, dos computadores e das redes de dados empregadas para interligá-los, fez surgir um ambiente virtual, sem fronteiras, denominado Espaço Cibernético[1]. O uso crescente deste espaço, em tempo de paz, na realização dos mais diferentes serviços, ocasionou o desenvolvimento dos chamados crimes cibernéticos, que se caracterizam pela prática de delitos contra os usuários da internet, aproveitando-se das vulnerabilidades existentes na mesma. Com o passar do tempo, tais técnicas desenvolvidas aparentemente para obter vantagens financeiras de cidadãos ou empresas civis, passaram a ser empregadas pelos Estados como armas de guerra surgindo, desta forma, o conceito de G Ciber.

Partindo-se do princípio que informações relevantes de combate vêm, de forma crescente, trafegando pelo espaço cibernético, a mercê daqueles que tiverem capacidade de interceptá-las, o estudo da G Ciber é uma necessidade improrrogável, especialmente ao se considerar a rapidez com que as novas tecnologias vêm se desenvolvendo.

Dentro desse contexto, este trabalho analisa a influência da G Ciber nos sistemas de C2 em apoio às Operações Militares (Op Mil). Para isso, inicialmente, são apresentados os conceitos relacionados ao tema, bem como as características dos sistemas de C2 baseados em rede. Em seguida, são discutidas as principais vulnerabilidades dos diferentes sistemas que se utilizam de redes de dados e as formas como essas vulnerabilidades podem ser exploradas por atacantes. A partir dessa análise, são apresentadas as principais medidas de proteção cibernética a serem empregadas no caso de ataques desencadeados contra sistemas baseados em redes de dados. Partindo-se do princípio que os atuais sistemas de C2 empregados em apoio às Op Mil estão cada vez mais conectados por intermédio de redes de dados, o estudo prossegue analisando as vulnerabilidades desses sistemas e as consequências de ações cibernéticas desencadeadas contra eles. Por fim, o presente trabalho propõe possíveis contramedidas a serem adotadas em tais ações.

2. Conceitos Importantes

2.1 Guerra Cibernética

"O ambiente cibernético pode ser considerado um novo domínio ou palco de batalha, depois da terra, do mar, do ar, do espaço exterior e do espectro eletromagnético" [2].

Em guerras anteriores, componentes críticos de infraestrutura, como aeroportos, usinas de energia, sistemas de água, ferrovias, oleodutos, gasodutos e centros de comunicações se tornaram alvos pelo fato de sua destruição poder paralisar toda uma Nação. Estes mesmos componentes já não precisam mais ser fisicamente destruídos, porque a maioria deles é dependente de sistemas baseados em redes

[1] Conjunto de pessoas, empresas, equipamentos e interconexões dos sistemas de informação e das informações que por eles trafegam [4].

de computadores, os quais se tornam alvos em potencial de ataques cibernéticos [3].

O conceito de "Paralisia Estratégica", defendido por Sun Tsu, vem se tornando uma forte tendência dos atuais combates assimétricos e se aplica muito bem ao conceito de G Ciber. Por intermédio de ações cibernéticas bem executadas, torna-se possível "paralisar" inimigos militares, numérica e economicamente superiores, sem ter que enfrentar, no terreno, seu poderio bélico.

As vulnerabilidades existentes na internet, no entanto, não abrem caminho somente para os Estados travarem guerras entre si. Pessoas comuns podem deflagrar guerras entre Estados, simplesmente manipulando os dados cibernéticos disponíveis no espaço e agindo às escuras, fazendo com que o país atacado tome conclusões errôneas sobre as origens dos ataques desferidos contra ele.

Além disso, países têm se utilizado desses cidadãos para mascarar suas participações em ataques cibernéticos. Ao mesmo tempo em que financiam suas ações, se negam a assumi-las, fazendo o mundo crer que foram feitas de forma isolada e sem um fim político específico.

É importante destacar que os resultados de um ataque cibernético dependem da integração das estruturas críticas do país à internet e, quanto mais uma Nação estiver integrada tecnologicamente, mais destruidor pode ser esse ataque [4].

Muito recentemente, um grupo de especialistas em tecnologia e ataques virtuais publicou um manual sobre *G Ciber*, determinando regras e normas de conduta para ataques cibernéticos. O manual Tallinn, que recebeu este nome em homenagem à capital da Estônia, local onde foi compilado, foi desenvolvido a pedido do Centro de Excelência em Defesa Cibernética Colaborativa da OTAN e aplica regras de comportamento de campos de batalha reais à internet. Seu objetivo é mostrar que uma guerra no mundo virtual pode se tornar real e, sendo assim, suas ações têm que ser submetidas às mesmas normas internacionais que regulam os combates nos campos de batalha.

Diariamente são registrados inúmeros ataques ou tentativas de intrusões em diversos sistemas espalhados ao redor do mundo e tais fatos corroboram para o acréscimo da importância do tema na agenda mundial, com diversos países e organizações internacionais preocupados com a implantação de estruturas e estratégias de defesa e segurança cibernética.

No Brasil a situação não é diferente. Em junho de 2011, diversos portais governamentais brasileiros, como o da Presidência da República, da Receita Federal e da Petrobras, foram alvos de ataques cibernéticos assumidos pelo grupo Lulz Security Brazil. Segundo o próprio grupo divulgou no Twitter, este ataque teria sido um protesto contra a corrupção e o aumento dos combustíveis. No mesmo período, o grupo Fatal Error Crew, que já havia atacado o portal da Presidência em janeiro de 2011, divulgou o endereço de 500 portais de prefeituras e câmaras municipais atacadas [2].

Diante de tais fatos e de medidas práticas adotadas pelo governo brasileiro, novas políticas e documentos têm sido criados e aprovados, com vistas a definir uma política cibernética para o país: a Estratégia Nacional de Defesa [5], o Livro Verde sobre Segurança Cibernética no Brasil [6]e a recente Política Cibernética de Defesa [7]. Também encontra-se em fase de aprovação no Ministério da Defesa (MD), a proposta de Doutrina Militar de Defesa Cibernética.

2.2 Sistemas de C2 baseados em redes

Dentre diversos setores, o militar foi um dos que teve que se adaptar ao surgimento da internet e ao crescimento exponencial das redes de dados, como uma potente ferramenta de trabalho. O processo de transformação militar iniciou-se tendo como base dois eixos principais: um voltado para a compreensão dos desafios do século XXI e outro focado no conceito de Guerra Centrada em Redes (GCR).

A GCR parte do princípio da integração dos diversos sistemas de apoio ao combate no intuito de se obter uma consciência compartilhada, com vistas a facilitar a tomada de decisão dos comandantes (Cmt) nos diversos níveis. Ela busca um maior grau de sincronização da informação, levando a um aumento significativo na agilidade e eficácia dos processos.

Na atualidade, pode-se dizer que C2 é a ciência e a arte que trata do funcionamento de uma cadeia de comando e que envolve, basicamente, três componentes fundamentais: a autoridade investida do comando, a sistemática do processo decisório e a estrutura para acompanhar as Op Mil [8].

A literatura em vigor, especialmente a norte-americana, trata C2 com a terminologia C4ISR: Comando, Controle, Comunicações, Computação, Inteligência, Vigilância (*Surveillance*) e Reconhecimento. No presente artigo, no entanto, optou-se pelo emprego do termo C2, por ser o mais comum e o adotado pelo Exército Brasileiro (EB).

Um novo modelo conceitual de C2, sugerido por um grupo de estudo da OTAN, tem servido de parâmetro para o entendimento de um processo de C2 mais amplo e que atenda às atuais necessidades dos combates modernos. Esse grupo concluiu recentemente que uma única abordagem não é suficiente para se alcançar o sucesso na missão, e que cada situação exigirá uma abordagem diferente, com base em três fatores-chave que definem a essência do C2. Esses três fatores podem ser considerados dimensões de uma Abordagem de C2 e são os seguintes:

- atribuição de direitos de decisão para o coletivo;
- padrões de interação entre os atores; e
- distribuição da informação

Dentro desta concepção mais moderna, a abordagem de C2 empregada por uma determinada Nação, coligação, ou força pode ser mais bem compreendida como uma região ou coleção de regiões dentro de um espaço tridimensional, ao invés de, um ponto dentro desse espaço.

Nesse contexto, e visando uma melhor compreensão das diferentes abordagens de C2 existentes, foram definidos cinco níveis de maturidade, os quais estão relacionados a essas abordagens e sua localização dentro do espaço tridimensional. São eles: Conflituoso, Não-conflituoso, Coordenado, Colaborativo e De ponta.

O grande problema é que, à medida que o nível de maturidade cresce, as interações aumentam e, por conseguinte, mais vulnerável o sistema de C2 se torna em função dos diferentes meios e ligações pelos quais as informações relevantes trafegam. Cabe, portanto, ao decisor escolher qual nível melhor se encaixa ao contexto da operação que irá executar lembrando-se que, o valor da informação está diretamente relacionado ao seu grau de segurança. Sendo assim, cresce de importância a proteção das informações e fontes de informação de uma variedade de ataques que podem ocorrer e prejudicar a eficiência dos sistemas de C2.

A teoria militar atual sugere que atacar os centros de gravidade[2] (CG) de uma Nação, além de suas Forças Armadas, é a maneira mais eficaz de destruir um inimigo em potencial. Sendo assim, os sistemas de C2 se tornaram o principal CG e, sua destruição, torna-se tão importante quanto destruir as forças militares de um adversário.

2.3 Vulnerabilidades em sistemas baseados em rede

Para executar ataques contra uma rede, um invasor normalmente adotará uma sequência lógica, que vai desde o levantamento dos dados necessários, passando pelas ações propriamente ditas, até a limpeza e exclusão dos rastros que porventura tenha deixado.

Para se proteger dessas ações, torna-se necessário conhecer profundamente tanto o ataque como a filosofia dos atacantes, pois, desta forma, será possível escolher a melhor contramedida a ser empregada.

A **Exploração Cibernética** consiste em ações de busca ou coleta nas redes de dados ou sistemas do inimigo, a fim de obter informações relevantes que podem ser empregadas em proveito da inteligência ou podem servir de subsídio para o planejamento de um ataque cibernético propriamente dito [10].

Durante a Exploração Cibernética, o atacante utiliza todas as ferramentas à disposição para levantar informações a respeito do alvo, explorando vulnerabilidades na infraestrutura de sua rede de dados, em algum software e/ou servidor, ou em erros de contrainteligência dos operadores e/ou administradores. Para atingir tal objetivo, a exploração poderá fazer uso, inclusive, de técnicas de invasão, desde que não causem danos ou prejuízos aos sistemas e redes de dados do oponente.

Já o **Ataque Cibernético** é mais agressivo e, por intermédio dele, o atacante conseguirá derrubar ou corromper total ou parcialmente redes de dados e sistemas do oponente, danificar equipamentos e dispositivos ou destruir bancos de dados e informações relevantes, podendo para isso, fazer ou não uso de técnicas de invasão.

Existem formas de ataque que podem ser empregadas diretamente contra determinados servidores, com o intuito de causar-lhes danos, ou mesmo derrubá-los totalmente, como é o caso de ataques direcionados a servidores Web ou a servidores de bancos de dados.

Já os vírus são ferramentas agressivas, muito disseminadas em ataques, com a finalidade de causar danos a um sistema-alvo. Eles são trechos de código que se anexam a um programa ou arquivo, de forma a poder se espalhar e infectar outros sistemas. Seus efeitos são bastante variados, podendo causar ou não danos ao sistema atacado. Como forma de atuação, sua maioria pode ser anexada a arquivos executáveis, podendo estar presente no computador sem, no entanto, provocar efeitos maliciosos, a menos que o programa ao qual esteja atrelado seja executado. É importante notar que eles não se espalham sem a ajuda de intervenção humana. Usuários desavisados acabam por disseminá-los, sem saber, através do compartilhamento de arquivos contaminados ou seu envio anexados a e-mails.

Atualmente os *Worms* ou Vermes são uma praga bastante empregada, pois residem na memória ativa do computador e se replicam automaticamente. Quando instalados na máquina, consomem muitos recursos dela, degradando sensivelmente o desempenho de redes e sobrecarregando seu disco rígido, devido à grande quantidade de cópias de si mesmo que costumam propagar.

Os *rootkits* são ferramentas mais modernas que têm causado danos irreversíveis a computadores e redes de dados. Esse tipo de arquivo malicioso, instalado muitas vezes de forma imperceptível, pode contaminar tarefas e processos da memória do Sistema Operacional (SO), proporcionando mensagens de erro. Ele tem a capacidade de se espalhar por diversos outros arquivos da máquina, produzindo danos contra seus programas, hardware e arquivos.

Mais recentemente, a Engenharia Social tem sido uma técnica de ataque bastante eficaz. Por intermédio dela, tenta-se ludibriar a vítima para que acredite nas informações prestadas e se convença a executar alguma tarefa e/ou aplicativo que venha a causar danos ao computador ou à rede como um todo. É importante destacar que, nesse tipo de ataque, a principal vulnerabilidade é a vítima, que não possui a devida conscientização sobre os perigos de acreditar em todas as informações que chegam até ela.

Diferentemente da maioria dos ataques existentes, o Ataque de Negação de Serviço ou *Denial of Service* (DoS) é um exemplo de ataque que não utiliza técnicas invasivas contra computadores, redes ou sistemas e nem mesmo modifica o conteúdo armazenado neles. Tal ataque tem como objetivo tornar inacessíveis os serviços providos pelo alvo aos seus usuários legítimos. Nenhum dado é roubado, nada é alterado e não ocorre nenhum acesso não autorizado ao computador do oponente. A vítima simplesmente para de oferecer o seu serviço aos clientes legítimos, enquanto tenta lidar com o tráfego gerado pelo ataque [11].

Outra forma de ataque, que não pode ser descartada, é aquela que faz uso das ferramentas de Guerra Eletrônica (GE). Por intermédio das Medidas de Apoio de Guerra Eletrônica (MAGE) o invasor pode detectar centros de C2 que estejam trafegando dados em redes sem fio e, de posse das informações técnicas levantadas a respeito da transmissão eletromagnética, pode utilizar as Medidas de Ataque Eletrônico (MAE) para realizar uma interferência ou mesmo um bloqueio nesse meio de transmissão. Este tipo de estratégia também pode ser usada para interferir ou mascarar sensores utilizados pelos Centros de C2. Assim, informações, tais como: posição, velocidade, temperatura, entre outras, podem ser modificadas de acordo com o interesse do atacante.

Ademais, os próprios sensores podem ser fisicamente alterados, pois, muitas vezes, estes sensores não recebem a mesma atenção dada ao restante dos sistemas de C2.

2.4 Proteção para vulnerabilidades dos sistemas baseados em redes

Quando se fala em termos de proteção em rede de dados, a primeira coisa a se reconhecer é que não há nenhuma ferramenta que proporcione 100% de eficácia. Obter o equilíbrio correto entre utilização e segurança torna-se uma tarefa difícil nos complexos e modernos sistemas. Se, numa análise inicial, um administrador de rede aceitar a premissa de que a segurança perfeita é inexequível, a principal estratégia por trás de um bom projeto de contramedidas se torna simples: aumentar o "custo" de um ataque, de modo que o investimento nele se torne alto demais em comparação com o ganho

[2] Centro de Gravidade (CG) é o ponto essencial de um Estado, de forças militares ou de sistemas diversos, cujo funcionamento é imprescindível à sobrevivência do conjunto. Os CG não se limitam a forças militares e servem como fonte de energia que fornece força moral ou física, liberdade de ação ou vontade de agir [9].

obtido pelo invasor [12].

Para se atingir a proteção de sistemas baseados em redes de dados, inicialmente, três verbos são fundamentais no planejamento de contramedidas: prevenir, detectar e responder. Desta forma, todo e qualquer plano de resposta a ataques cibernéticos deve conter medidas preventivas, que incluem ações de prevenção e detecção de vulnerabilidades e medidas repressivas, que são as respostas propriamente ditas aos incidentes.

Um plano de contramedidas também pode ser estruturado com base na proteção pelas cinco camadas de TI, quer sejam: física, rede, host ou computador, aplicação e lógica. Por intermédio desse tipo de estratégia torna-se possível corrigir vulnerabilidades em cada ponto de junção, impondo barreiras às diferentes formas de invasão.

3. Levantamento de ações cibernéticas típicas e seus impactos em sistemas de C2 em rede

C2 é fundamental para o êxito das Op Mil em todos os níveis de comando. Ele é responsável pela sincronização de todas as atividades operacionais e de apoio, permitindo ao Cmt adquirir e manter a indispensável Consciência Situacional[3] que lhe dará o suporte para a tomada de decisões adequadas e oportunas.

Sabe-se que para atuar em um ambiente cibernético, normalmente o atacante executará uma sequência de ações visando coletar dados e obter acesso à rede de seu oponente. O conjunto dessas ações pode ser dividido em duas grandes fases: **Exploração Cibernética** e **Ataque Cibernético**. No caso de ataques contra sistemas de C2, a sequência empregada é praticamente a mesma, uma vez que os sistemas modernos são quase que totalmente baseados em redes de computadores.

Inicialmente, o atacante buscará levantar o perfil de seu alvo, coletando informações disponíveis, especialmente na internet. O site institucional do alvo muitas vezes poderá fornecer informações relevantes. Nele o atacante poderá localizar páginas específicas que façam referências ao sistema de C2 adotado. Pesquisando mais a fundo na internet, poderá localizar manuais, documentos, vídeos e até apresentações sobre o funcionamento desse sistema. Muitas vezes, em tempo de paz, palestras ministradas em quarteis são disponibilizadas na internet, por um elemento desavisado, que por algum motivo deixou de cumprir as normas de Segurança da Informação.

Coletando as informações a respeito do alvo, o atacante poderá realizar a varredura em sua rede. Nesse momento, procurará identificar computadores ativos e portas TCP abertas. Nas operações de combate, especialmente nos níveis operacional e tático, um sistema de C2 em apoio a uma Força Terrestre Componente[4] (FTC) ou qualquer outra força similar, provavelmente será desdobrado no terreno empregando a infraestrutura militar disponível. Normalmente, a interconexão das redes ocorrerá por meio físico, rádio ou por micro-ondas com visada direta. Realizar varredura em redes locais, isoladas no terreno, não é algo simples. Ela pode ser feita por intermédio do emprego de equipamentos de GE, caso o atacante consiga interceptar o sinal rádio e explorá-lo, ou por meio de qualquer conexão física local. Nesse momento, crescem de importância as Medidas de Proteção Eletrônica[5] (MPE) e as medidas de segurança dos equipamentos e instalações físicas, especialmente dos dispositivos móveis empregados.

Embora muitas vezes as redes de C2 estejam segregadas à área ou Teatro de Operações (TO), a força desdobrada no terreno necessita se conectar ao sistema do escalão superior. Esta conexão pode ser feita de muitas maneiras e, uma delas, ocorre por meio do estabelecimento de uma Rede Privada Virtual ou *Virtual Private Network* (VPN)[6]. Além disso, os sistemas de C2 atuais são muito complexos e muitas de suas ferramentas necessitam coletar informações disponíveis na internet para complementar os dados constantes em seus bancos de dados. O atacante tentará, então, explorar estas portas de acesso à internet e o êxito de suas ações de varredura dependerá do nível de conectividade do sistema C2 do alvo – quanto mais conectado ele estiver à internet, mais facilidade o atacante terá de levantar informações a seu respeito.

Coletando as devidas informações da rede de C2 do alvo, o atacante poderá avançar para a próxima etapa: realizar a enumeração. Nesta ação, ele buscará identificar o Sistema Operacional (SO) do servidor da rede de C2 do alvo, os SO e os dados dos usuários dos computadores ativos na rede, os recursos compartilhados mal configurados e as versões de software com vulnerabilidades de segurança que poderão ser exploradas. Ao término da Enumeração, o atacante terá todas as ferramentas necessárias para intrusão na rede de dados em que o sistema C2 do alvo está operando. Todas as informações colhidas serão processadas pela célula funcional Inteligência, servindo para complementar os dados das outras fontes e auxiliar no planejamento de ações futuras.

Considerando que a maioria dos sistemas de C2 está instalada em plataformas *Windows* ou *Linux* e visando obter o acesso a tais SO, o atacante passará a empregar técnicas específicas para realizar a invasão desses sistemas por intermédio de *software*, hardware ou conexão, de acordo com o que foi identificado durante a ação de enumeração. Nesse instante, ele buscará o acesso inicialmente como usuário comum da rede e, posteriormente, tentará elevar seus privilégios até conseguir permissões de administrador.

Atingindo esse nível de intrusão, o invasor poderá optar por não executar, de imediato, um ataque propriamente dito, prosseguindo com a Exploração Cibernética que vinha realizando desde o levantamento do perfil. Sendo assim, passará a vasculhar toda a rede, bem como o sistema C2 e seus bancos de dados, coletando o máximo de informações possíveis, tanto do servidor quanto dos usuários. Ele também poderá instalar um *backdoor*, para garantir um fácil acesso à rede e ao siste-

[3] Consciência Situacional consiste na percepção atualizada do ambiente operacional no qual se atuará e no reconhecimento da importância de cada elemento percebido em relação à missão atribuída. Ela garante a decisão adequada e oportuna em qualquer situação de emprego, permitindo que os Cmt possam se antecipar aos oponentes e decidir pelo emprego de meios na medida certa, no momento e local decisivos, proporcionalmente à ameaça. Quanto mais acurada a percepção que se tem da realidade do ambiente operacional, melhor a Consciência Situacional [13].

[4] A FTC é o comando singular responsável pelo planejamento e execução das operações terrestres, no contexto de uma operação conjunta. Possui constituição e organização variáveis, enquadrando meios da Força Terrestre adjudicados ao Comando Operacional, bem como de outras Forças Singulares necessários à condução das suas operações [14].

[5] Medidas de Proteção Eletrônica (MPE): Ramo da Guerra Eletrônica que busca assegurar a utilização eficaz e segura das próprias emissões eletromagnéticas, a despeito das ações de GE empreendidas pelo oponente ou formas de interferências não intencionais [15].

[6] VPN é um conceito amplo que envolve a cifração e o "tunelamento"de dados privados pela internet. A técnica de tunelamento consiste em encapsular um protocolo dentro do outro, proporcionando maior segurança, redução de custos e conveniência [12].

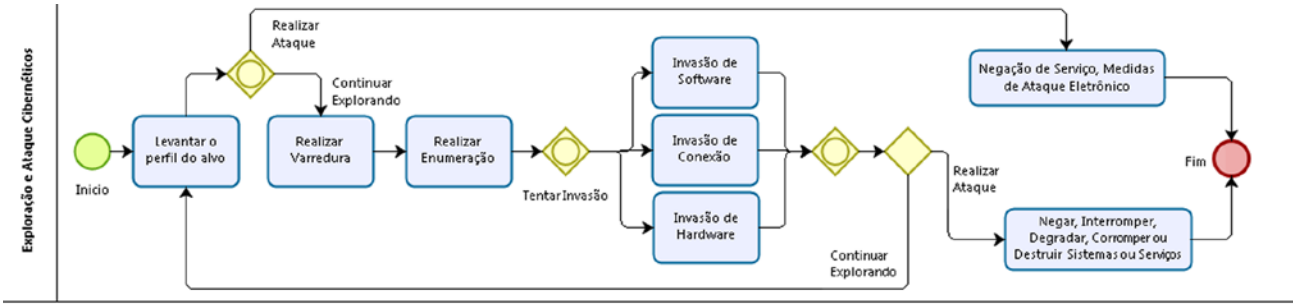

Fig. 1 – Sequência de Ações nas Fases de Exploração e Ataque Cibernéticos

Fig. 2 – Impactos de ações cibernéticas contra um sistema de C2

ma, visando explorações futuras ou mesmo para desencadear um ataque comandado remotamente.

Resumidamente, na fase de Exploração Cibernética, o atacante poderá: levantar o perfil, realizar a varredura, realizar a enumeração e realizar a invasão de software, hardware ou conexão, procurando ocultar suas ações e evitar o rastreamento.

Mas o invasor poderá também ter a intenção de agir ofensivamente. Desta forma, realizará um Ataque Cibernético contra o servidor de rede do alvo, desestabilizando a rede de C2 como um todo ou mesmo derrubando-a. Ele também poderá optar por atuar somente contra determinado banco de dados, previamente identificado, corrompendo-o ou mesmo excluindo-o totalmente. Além disso, o invasor poderá ter colhido informações suficientes que lhe permitam penetrar no sistema C2 propriamente dito, causando danos irreversíveis a todo o processo de tomada de decisão.

Desta feita, na fase de Ataque Cibernético, o atacante poderá, resumidamente: realizar o ataque de modo a negar, interromper, degradar, corromper ou destruir o funcionamento do sistema ou serviço que foi alvo da intrusão.

A Exploração e o Ataque Cibernéticos podem ser vistos como um grande processo formado por diversas tarefas e/ou ações. Portanto, visando maior compreensão deste processo, optou-se por representar a sua sequência de ações típicas por meio da notação de processos, utilizada na área de Gerenciamento de Processos de Negócios (*Business Process Management - BPM*)[7] . Nesta notação, os círculos no inicio e no fim do diagrama indicam o início e o fim do processo ou subprocesso. Os retângulos com cantos arredondados indicam tarefas, atividades ou ações. Se os retângulos possuírem em seu interior um sinal de positivo, indicam subprocessos. Os losangos vazios com uma entrada e duas ou mais saídas indicam um desvio do fluxo de atividades em que apenas um dos caminhos de saída será seguido. Os losangos vazios com duas ou mais entradas e uma saída indicam uma convergência de fluxos em que o primeiro fluxo a chegar dará continuidade ao fluxo do processo, não sendo necessário esperar pelos demais fluxos. Estes tipos de desvios são conhecidos como portas ou desvios exclusivos. Os losangos com um círculo no centro e com uma entrada e duas ou mais saídas indicam que o fluxo pode seguir por um ou mais de um caminho de saída ao mesmo tempo (fluxo único ou fluxos paralelos). Os losangos com um círculo no centro e duas ou mais entradas e uma saída indicam que o processo só seguirá adiante depois que todos os fluxos de atividades em execução sejam concluídos.

Entre as vantagens de formalizar o processo de Exploração e Ataque Cibernéticos com a notação de Gerenciamento de Processos de Negócios, podem ser destacadas: a possibilidade de automação do processo, onde for possível, e a possibilidade de envio de mensagens de alerta e solicitações de checagem, quando for necessária a intervenção humana. Assim, sistemas de proteção cibernética podem atuar de acordo com a sequência lógica de ações que um atacante executa, buscando maximizar a eficiência das medidas de proteção.

A Fig. 1 apresenta a sequência de ações tipicas de um atacante a um sistema de C2. A maioria destas ações são as mesmas de qualquer sistema em rede de computadores, permitindo que a análise realizada neste trabalho também seja aplicada a estes sistemas. Entretanto, alguns pontos no contexto de C2 merecem especial atenção e podem diferir dos sistemas tradicionais, a exemplo das Medidas de Ataque Eletrônico (MAE) e da invasão de Hardware envolvendo sensores de C2. É importante considerar que são apresentadas as sequências de ações típicas de um ataque, podendo ocorrer variações no fluxo de atividades. Porém, estas variações não comprometem o levantamento das proteções cibernéticas que serão apresentadas na próxima Seção.

[7] Disponível em: <http://www.bpmn.org/>. Acesso em: 06 abr. 2015.

A Fig. 2 representa as consequências de ações cibernéticas desencadeadas contra sistemas de C2. A partir de sua interpretação, pode-se inferir que um ataque cibernético bem sucedido poderá causar falhas consideráveis no tráfego da informação dentro do processo de C2. Estas falhas, por sua vez, poderão acarretar informações sem qualidade, ou mesmo total falta delas. Isto causará impactos profundos na qualidade do C2, prejudicando a formação da Consciência Situacional e o processo de tomada de decisão. Os principais reflexos serão sentidos na "ponta de linha", pois as tropas terão dificuldades em cumprir suas missões, devido à sua baixa efetividade operacional.

Por se tratar de um ciclo, as ações e reações serão repetidas durante todo o processo de C2 e, enquanto o ataque cibernético estiver sendo eficaz, as informações serão geradas com perda crescente de qualidade e agilidade, o que prejudicará sobremaneira as tomadas de decisão futuras.

Assim, para impedir que ataques dessa natureza interrompam ou dificultem a interconectividade dos sistemas de C2 desdobrados em apoio à determinada Op Mil, ou mesmo para impedir que o atacante realize Exploração Cibernética, há que se considerar as medidas de proteção das redes e sistemas.

4. Possíveis contramedidas em sistemas de Comando e Controle

Garantir a Superioridade de Informação (SI)[8] é a principal missão da Proteção Cibernética. Ela abrange todas as ações necessárias para proteger as redes de dados e de C2 contra os ataques desencadeados pelo oponente e compreende a proteção contra a interrupção, negação, degradação ou destruição das informações que por elas trafegam.

Tendo em vista o aumento crescente de ações cibernéticas contra redes e sistemas, a Segurança Criptográfica tem adquiro cada vez mais importância na atualidade. Ela consiste no emprego de processos de codificação ou criptografia para alterar o conteúdo original da informação, de modo a torná-la incompreensível.

O ideal é que a criptografia seja empregada tanto na proteção da infraestrutura que dará suporte à rede de C2, realizando a cifração do link de dados entre os diferentes escalões de comando, quanto no nível de usuário, criptografando as informações operacionais relevantes ao combate.

Ressalta-se que o sucesso na Proteção Cibernética dos sistemas de C2 baseados em rede está calcado na combinação de todas as técnicas e processos de segurança, de forma a reduzir, ao máximo possível, as chances de invasão e de vazamento de informações.

O emprego de todas as ferramentas e procedimentos de segurança disponíveis, somado a uma boa auditoria, são a mistura certa para a eficiência do trabalho do administrador de redes de C2.

Torna-se importante, no entanto, em todo e qualquer tipo de planejamento relacionado à G Ciber, jamais se esquecer de uma de suas características básicas - a Insegurança Latente – que parte do princípio que nenhum sistema computacional é 100% seguro, uma vez que sempre será objeto de exploração por ameaças cibernéticas. Assim, os planos de contramedidas e de contingência jamais devem ser relegados, sendo de fundamental importância sua confecção nos diferentes níveis.

Os Planos de Contingência devem contemplar os diferentes tipos de ataque possíveis de ocorrer. Dessa forma, cada administrador de rede e/ou sistema saberá como agir, com rapidez e eficácia, diante de cada situação apresentada, mantendo a resiliência necessária para que todos os usuários sofram o mínimo possível os impactos das ações desencadeadas.

A Fig. 3 expande e ilustra as ações cibernéticas já mostradas na Fig. 1, que podem ser desencadeadas contra redes de dados e, consequentemente, contra sistemas de C2 com estruturas baseadas em tais redes, bem como algumas das principais medidas de Proteção Cibernética que podem ser adotadas. A Fig. 3 contém dois subprocessos: Invasão e Contramedidas contra a Invasão, detalhado na Fig. 4, e

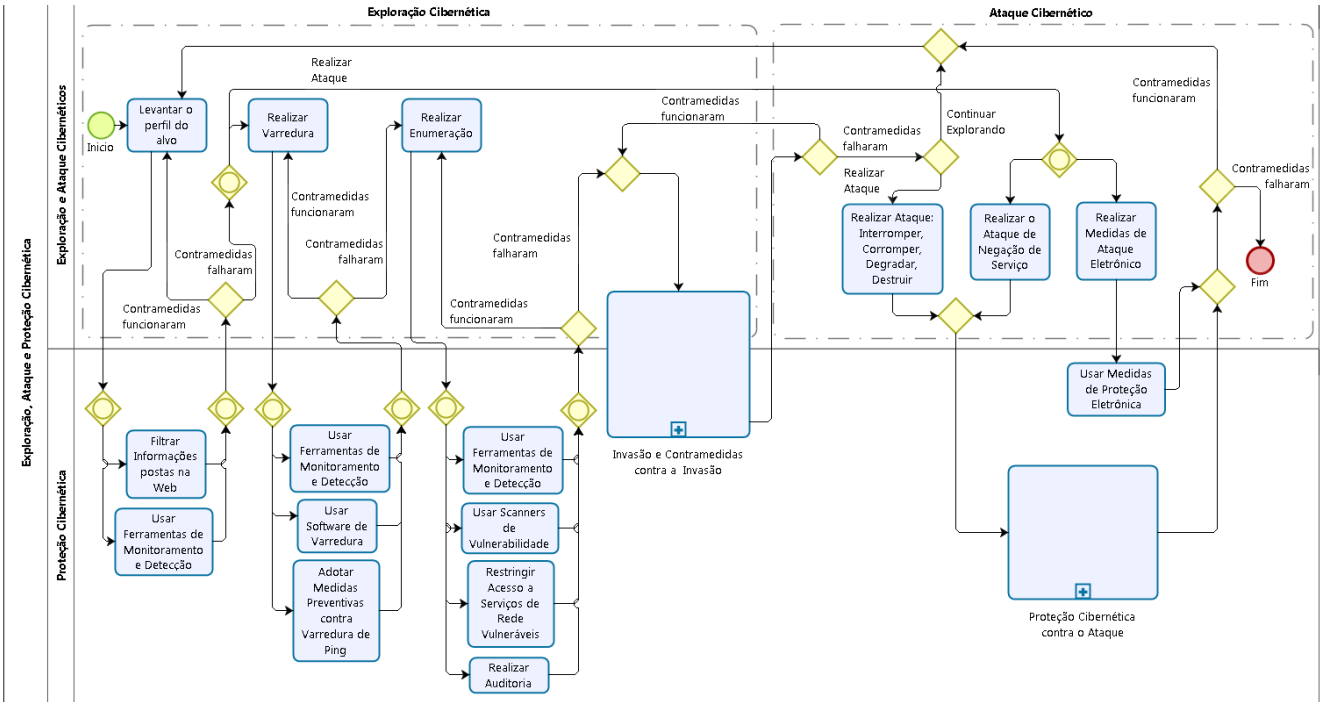

Fig. 3 - Sequência de Ações e Proteções Cibernéticas nas Fases de Exploração e Ataque Cibernéticos

[8] Superioridade da Informação (SI) é a capacidade de fornecer informações pertinentes aos usuários interessados, no momento oportuno e no formato adequado, negando ao adversário as oportunidades de atingi-la [8].

Proteção Cibernética contra o Ataque, detalhado no Fig. 5.

5. Conclusão

Num momento em que os sistemas de C2 estão cada vez mais conectados em rede, a G Ciber vem despontando com um potencial considerável. Suas ações podem desestruturar esses sistemas e prejudicar a tomada de decisão precisa e oportuna. Desta maneira, conhecer suas formas de ataque e defesa permite identificar contramedidas que possam ser tomadas no intuito de reduzir, ou pelo menos eliminar, os seus efeitos sobre os sistemas de C2.

Esse trabalho se propôs, a partir de um estudo mais aprofundado das medidas de ataque e proteção cibernética, apresentar uma sequência de ações típicas dos atacantes e uma proposta das correspondentes proteções cibernéticas que podem ser adotadas, conforme exposto nas Fig. 3, 4 e 5. Este processo foi modelado através da notação de Gerenciamento de Processos de Negócios, o que pode facilitar a automação, onde for possível, e a possibilidade de envio de mensagens

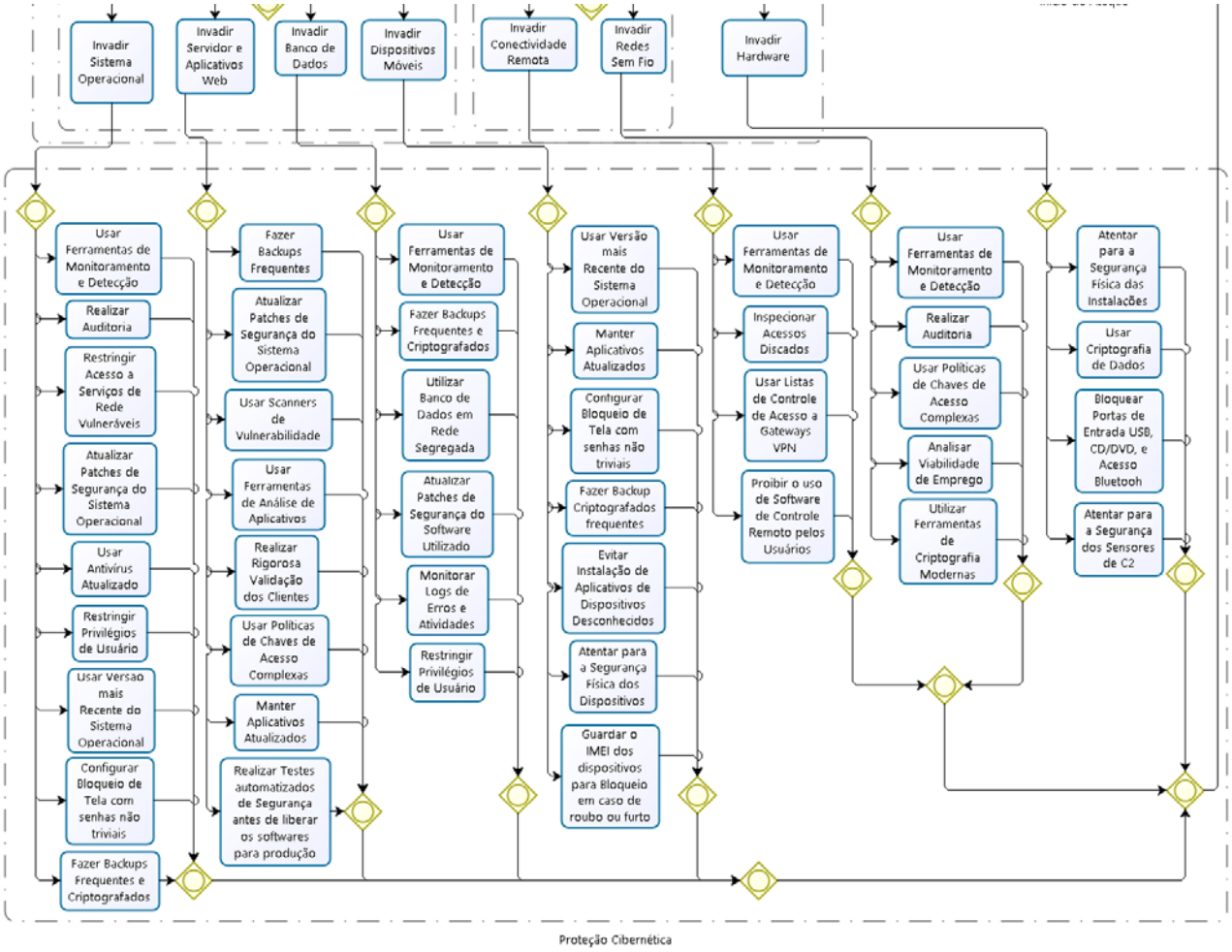

Fig. 4: Sequência de Ações e Proteções Cibernéticas na Fase de Invasão

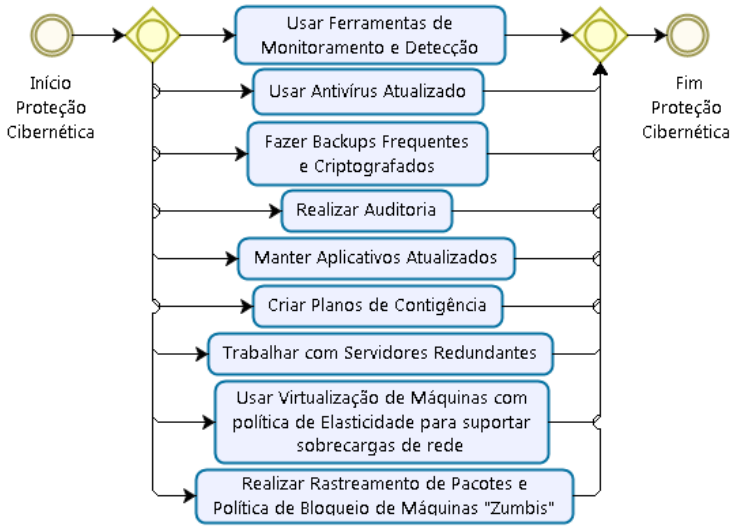

Fig. 5: Proteções Cibernéticas na Fase de Ataque

de alerta e solicitações de checagem, quando for necessária a intervenção humana.

Por fim, em que pese as vulnerabilidades e possibilidades apresentadas é fato que o Brasil, e em especial o EB, tem avançado muito rápido no setor cibernético o que pode ser comprovado pelos avanços nas legislações e normas recentemente criadas. Como referência adicional sobre o assunto, ver [16-23]. Até pouco tempo atrás, quase nada havia de concreto em termos de Segurança Cibernética. Em curto espaço de tempo, muitas ações vêm sendo desenvolvidas e, com certeza, novas formas de proteção serão incorporadas aos softwares de C2, tudo com o intuito de protegê-los cada vez mais de novos ataques surgidos diariamente.

Referências Bibliográficas

[1] ALBERTS, David S; HAYES, Richard E. Understanding Command and Control. CCRP, 2006.

[2] SALDAN, Eliane. Doutrina precisa definir guerra cibernética. Disponível em: <http://www.conjur.com.br/2011-ago-06/guerra-cibernetica-urgentemente-definicao- doutrina>. Acesso em: 5 fev. 2014.

[3] KAMAL, A. The Law of Cyber-space - an invitation to the table of negotiations. 1a. ed. Suiça: UNITAR - United Nations Institute of Training and Research, 2005.

[4] MANDARINO JUNIOR, R. Segurança e Defesa do Espaço Cibernético Brasileiro (2010 - Edição 1) - Cia. dos Livros. 1. ed. [s.l: s.n.].

[5] BRASIL. Decreto Nº 6.703, de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defesa, e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 19 de dezembro de 2008.

[6] _____. Presidência da República. Livro Verde de Segurança Cibernética no Brasil 1. ed. Brasília, DF, 2010.

[7] _____. Ministério da Defesa. Política Cibernética de Defesa - MD31-P-02. 1. ed. Brasília, DF, 2012.

[8] _____. Exército. Estado-Maior do Exército. EB20-MC-10.205: Comando e Controle. 1. ed. Brasília, DF, 2015.

[9] _____. Exército. Estado-Maior do Exército. EB20-MF-10.103: Operações. 4. ed. Brasília, DF, 2014c.

[10] Brasil. Ministério da Defesa. Doutrina militar de Defesa Cibernética (Proposta). 1. ed. Brasília, DF, 2013.

[11] MIRKOVIC, J., DIETRICH, S., DITTRICH, D., REIHER, P. apud LAUFER et al. Negação de Serviço: Ataques e Contramedidas. Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais, COPPE-Poli – UFRJ e Université Pierre et Marie Curie, p. 372.

[12] MCCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George. Hacking Exposed: Network Security Secrets and Solutions, 7th Edition. Bookman, 2012. VitalBook file.

[13] Brasil. Exército. Estado-Maior do Exército. EB20-MC-10.213: Operações de Informação. 1. ed. Brasília, DF, 2014b.

[14] _____. Exército. Estado-Maior do Exército. EB20-MC-10.202: Força Terrestre Componente. 1. ed. Brasília, DF, 2014a

[15] _____. Exército. Estado-Maior do Exército. C 34-1: Emprego da Guerra Eletrônica. 2. ed. Brasília, DF, 2009.

[16] ABNT. Associação Brasileira de Normas Técnicas. Tecnologia da Informação - Técnicas de Segurança – Código de prática para controles de Segurança da Informação (ABNT NBR ISO/IEC 27002:2013). Rio de Janeiro: ABNT, 2013. 99 p.

[17] ALBERTS, David S; HUBER, Reiner K.; MOFFAT, James. NATO NEC C2 maturity model. Washington: DoD Command and Control Research Program, 2010.

[18] CLARKE, Richard A.; KNAKE, Robert K. Cyber War: The Next Threat to National Security and What to Do About It. 1. Ed. Harpercollins, USA, 2010.

[19] FERREIRA, M. F. T. et al. Análise de vulnerabilidades em Sistemas Computacionais Modernos: Conceitos, Exploits e Proteções. Sociedade Brasileira da Computação, n. XII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais — SBSeg 2012, p. 50, 2012.

[20] LAUFER, Rafael P. et al. Negação de Serviço: Ataques e Contramedidas. Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, COPPE-Poli – UFRJ e Université Pierre et Marie Curie, p. 359-421, 2005.

[21] NEPTUNE, J. W. Cyber-Based C4ISR Asset: A U.S. Air Force Critical Vulnerability. [s.l.] BiblioScholar, 2012.

[22] VASSILIOU, Marius S.; ALBERTS, David S. C2 in Underdeveloped, Degraded and Denied Operational Environments - C2 Failures: A Taxonomy and Analysis. 18th ICCRTS, v. 18, p. 25, 2013.

[23] WALLACE, W. S. Comando em Combate habilitado para operações em rede. Military Review, n. Jul-Ago 2005, p. 6, 2005.