ISBN: 9788554844056

XXI CICLO DE ESTUDOS ESTRATÉGICOS

CIBERESPAÇO: A NOVA DIMENSÃO DO CAMPO DE BATALHA

Escola de Comando e Estado-Maior do Exército

"Sem um projeto de Nação definido, somente pelo acaso o Brasil logrará êxito: pensar estrategicamente esse gigante é condição sine qua non para que o Brasil consiga superar os seus desafios."

(Tenente-Coronel Anselmo de Oliveira Rodrigues, EBLOG - 2019)

XXI CICLO DE ESTUDOS ESTRATÉGICOS

CIBERESPAÇO: A NOVA DIMENSÃO DO CAMPO DE BATALHA

Organizadores

Coronel Carlos Eduardo de Franciscis Ramos

Coronel José Maria da Mota Ferreira

Coronel Ricardo Ribeiro Cavalcanti Baptista

Tenente-Coronel Anselmo de Oliveira Rodrigues

Este material é fruto da compilação das degravações referentes às apresentações orais realizadas nas diversas conferências, painéis e mesas temáticas, conjugadas com as apresentações em slides e textos oferecidos pelos autores, por ocasião da realização do XXI Ciclo de Estudos Estratégicos.

ECEME

2019

C567c XXI Ciclo de Estudos Estratégicos - Ciberespaço: a nova dimensão do campo de batalha/organizadores: Coronel Carlos Eduardo de Franciscis Ramos, Coronel José Maria da Mota Ferreira, Coronel Ricardo Ribeiro Cavalcanti Baptista, Tenente-Coronel Anselmo de Oliveira Rodrigues. - Rio de Janeiro: ECEME, 2019.

199 p. Inclui bibliografia

ISBN 978-85-64844-05-6

1. Ciberespaço. 2. Cibernética. 3. Defesa. 4. Exército Brasileiro. 5. Comunicação estratégica. 6. Operações de informação

CDD 303.483

Comandante do Exército Brasileiro
General de Exército Edson Leal Pujol

Chefe do Departamento de Educação e Cultura do Exército
General de Exército Miguel Miné Ribeiro Paiva

Diretor de Educação Superior Militar
General de Divisão João Batista Bezerra Leonel Filho

Comandante da Escola de Comando e Estado-Maior do Exército
General de Brigada Rodrigo Pereira Vergara

Subcomandante da Escola de Comando e Estado-Maior do Exército
Coronel Wellington Silva Lousada

Chefe do Instituto Meira Mattos
Coronel Carlos Eduardo de Franciscis Ramos

ECEME

2019

SUMÁRIO

Apresentação..... 6
Coronel Carlos Eduardo de Franciscis Ramos

Palavras de abertura. 8
General de Brigada Rodrigo Pereira Vergara

***Ciberespaço*: a nova dimensão do campo de batalha..... 9**
General de Exército José Luiz Dias Freitas

A Comunicação Estratégica do Exército e a Dimensão Informacional. 22
General de Divisão Richard Fernandez Nunes

Setor Estratégico do Cibernético. 30
General de Divisão Guido Amin Naves

***Ciberespaço* no contexto da Guerra do Futuro: uma visão da academia. 45**
Avelino Francisco Zorzo

A Cibernética sob a perspectiva operacional e empresarial..... 56
Roberto Alves Gallo Filho

O domínio da narrativa nas Operações de Informação e os Ataques Cibernéticos 65
Tenente-Coronel Alexandre Santana Moreira

O domínio da narrativa na manutenção do poder aeroespacial 79
Brigadeiro Pedro Arthur Linhares Lima

Centro de Defesa Cibernética..... 88
General de Brigada Alan Denilson Lima Costa

O Comando de Comunicações e Guerra Eletrônica do Exército (CCOMGEX) 99
General de Brigada Carlos Alberto Dahmer

Operações de Inteligência e de Informações no contexto da Guerra Cibernética. 113
Coronel Miler Barbosa das Neves

A Cibernética sob a Perspectiva Geopolítica. 121
Ricardo Borges Gama Neto

Proteção de Infraestruturas Críticas contra Ataques Cibernéticos 126
Alisson Campos Raposo

Políticas Públicas de Defesa Cibernética em Perspectiva Comparada: uma análise dos casos de EUA, China, Rússia e Israel..... 138
Dannielle Jacon Ayres Pinto

***Cibersegurança* ou *Ciberdefesa*? Conceitos e experiências em países diferentes.....147**
Daniel Oppermann

Políticas Públicas de Defesa Cibernética em Perspectiva Comparada - Argentina. 154
Major Mariano Oscar Gómez

***Cibersecurity* e Infraestruturas Críticas 162**
André Clark

Ciber Arena (ABDI-BIOTIC) 169
Larissa de Freitas Querino

Laboratório de Segurança Cibernética em ambiente de Tecnologia de Informação e automação aplicada em Sistemas Elétricos. 175
Tenente-Coronel Antônio Eduardo Carrilho da Cunha

***Strategic Perspectives on Cyberdefense* 181**
Joe Devanny

APRESENTAÇÃO

Coronel Carlos Eduardo de Franciscis Ramos*

A primeira edição da Estratégia Nacional de Defesa (END) em 2008 trouxe para a agenda de Defesa Nacional a necessidade de se desenvolver o setor cibernético, que juntamente com o setor nuclear e com o setor aeroespacial, foi apontado pela respectiva END como sendo um dos três setores estratégicos para o desenvolvimento do país. Dessa forma, coube ao Exército Brasileiro o desenvolvimento do setor cibernético. Diferentemente dos demais setores, o assunto era novo no Brasil. Após onze anos, notam-se diversos avanços no setor cibernético no país: a criação do Comando de Defesa Cibernética (ComDCiber) e do Centro de Defesa Cibernética (CDCiber) marcam o estabelecimento de estruturas voltadas para o nível tático e operacional, mas que também são capazes de gerar reflexos no nível estratégico.

De igual forma, observou-se no mesmo período o incremento do uso do *ciberespaço.* A forma dinâmica como evolui o setor implica em constante avaliação e aperfeiçoamento na capacitação de recursos humanos especializados, na criação de uma mentalidade cibernética na sociedade e na adoção de políticas públicas que possam estruturar o setor cibernético de forma transversal.

Em face disso, o tema vem sendo amplamente debatido na sociedade. O segmento militar coloca em evidência conceitos como guerra omnidimensional, operações multidomínio e guerra informacional. Nota-se a ocorrência de ataques cibernéticos (estatais ou não) em todas as partes do mundo. De fato, a arena cibernética engendra em si uma série de possibilidades inéditas em diversos ramos e atividades humanas, dentre estas a Defesa e a Segurança. Nesse sentido, a Escola de Comando e Estado-Maior do Exército (ECEME) vem contribuindo para o desenvolvimento de massa crítica e qualificada no setor cibernético.

É nesse contexto que foi realizado o ***XXI Ciclo de Estudos Estratégicos - Ciberespaço: A Nova Dimensão do Campo de Batalha,*** tema que possui total aderência e integração com os trabalhos desenvolvidos ao longo de 2019 referentes ao Projeto Interdisciplinar (PI) do Curso de Altos Estudos Militares, demandado pelo Comando de Operações Terrestres. Essa atividade foi organizada da seguinte forma; conferências, painéis temáticos e mesas temáticas.

* Doutor em Ciências Militares e Chefe do Instituto Meira Mattos.

Nas conferências foram abordados os assuntos centrais da dimensão Cibernética: ***"Ciberespaço como novo domínio de combate"***, proferida pelo General de Divisão Guido Amim Naves (Comando de Defesa Cibernética); e ***"A comunicação estratégica e a Dimensão Informacional"***, proferida pelo General de Divisão Richard Fernandez Nunes (Chefe do Centro de Comunmicação Social do Exército).

Nos painéis temáticos buscou-se diversificar os assuntos abordados nas conferências. Do lado militar, o General de Brigada Alan Denilson Lima Costa (Chefe do Centro de Defesa Cibernética) e o General de Brigada Carlos Alberto Dahmer (Comandante de Comunicações e Guerra Eletrônica do Exército Brasileiro) fizeram apresentações sobre ***"A Defesa Cibernética"***. E do lado acadêmico, o professor Joseph Devanny, da *King's College of London*, fez uma apresentação sobre as ***"Perspectivas estratégicas em ciberdefesa"***.

As mesas temáticas, por seu turno, foram montadas de forma a complementar o assunto central do Ciclo de Estudos Estratégicos. A mesa temática ***"Ciber no contexto da Guerra do Futuro: uma visão da academia"*** foi composta pelo Professor Avelino Francisco Zorzo (PUCRS) e por Roberto Alves Gallo Filho (Presidente da ABIMDE). Já a mesa temática ***"O Domínio da Narrativa nas Operações de Informação e os Ataques Cibernéticos"*** foi composta pelo Brigadeiro Pedro Arthur Linhares de Lima (UNIFA) e pelo Tenente- Coronel Alexandre Santana Moreira (Comandante do 1º Batalhão de Comunicações de Selva). A mesa temática ***"Operações de Inteligência e de Informações no contexto da Guerra Cibernética"*** foi composta pelo Coronel Miler Barbosa das Neves (Comandante do Centro de Inteligência do Exército), pelo Professor Ricardo Borges Gama Neto (UFPE) e pelo Oficial de Inteligência Alisson Campos Raposo (Agência Brasileira de Inteligência). A mesa temática ***"Políticas Públicas de Defesa Cibernética em Perspectiva Comparada"*** foi composta pela Professora Danielle Jacon Ayres (ECEME), pelo Professor Daniel Oppermann (ECEME) e pelo Major do Exército Argentino Mariano Oscar Gomez (ECEME). Finalizando, a mesa temática "***Cibersecurity e Infraestruturas Críticas"*** foi composta por André Clark (Presidente da Siemens do Brasil), pela Larissa de Freitas Querino (Coordenadora de Difusão Tecnológica da ABDI) e pelo Tenente-Coronel Antônio Eduardo Carrilho da Cunha.

Assim, a presente publicação disponibiliza para estudiosos e pesquisadores toda a gama de conhecimentos apresentados e debatidos durante o evento, na crença de que possa ser útil no referencial teórico do tema.

Boa leitura!

PALAVRAS DE ABERTURA
(Proferidas em 29 de julho de 2019)

Senhores oficiais-generais e autoridades já mencionadas no protocolo da Escola de Comando e Estado-Maior do Exército (ECEME), caríssimos integrantes da ECEME e caríssimos convidados. É com extrema satisfação e orgulho que vemos esse auditório cheio de pessoas que vieram em busca do conhecimento, da discussão de novas idéias e da atualização sobre um tema tão relevante para o setor de Defesa e para outros setores da vida nacional: a área cibernética.

De antemão, gostaria de trazer o nosso agradecimento ao General Freitas, ao General Arruda, ao Embaixador, Camilo Côrtes às demais autoridades aqui presentes, aos palestrantes e a todos que vieram e que dispuseram deste tempo para de alguma forma contribuir com o pensamento de Defesa na área cibernética.

A ECEME, como um dos instrumentos do Exército Brasileiro para a prospecção de conhecimento e doutrina, vem trabalhando no sentido de atender às demandas do Estado-Maior do Exército (EME) e do Comando de Operações Terrestres (COTER), advindas da Guerra do Futuro, num horizonte temporal de 2035.

Um dos setores mais relevantes e que interfere no combate do futuro é, justamente, o combate cibernético, que é a motivação do encontro de hoje. Também por esse motivo, agradecemos a presença do General Freitas, que se dispôs a encontrar um espaço em sua apertadíssima agenda para estar aqui conosco prestigiando esse evento, nos brindando com a abertura do nosso Ciclo de Estudos Estratégicos (CEE). General Freitas, tenha a certeza que a apresentação que o senhor nos trará hoje norteará os trabalhos do evento ao longo dos próximos três dias.

General de Brigada Rodrigo Pereira Vergara
Comandante da Escola de Comando e Estado-Maior do Exército

CIBERESPAÇO: A NOVA DIMENSÃO DO CAMPO DE BATALHA

General de Exército José Luiz Dias Freitas*

1. Introdução

Senhoras e senhores, boa tarde.

É motivo de grande satisfação retornar a esta casa, neste auditório, num evento tão especial para nós. Uma especial saudação para o meu companheiro do Alto Comando General Arruda, ao General Amim, ao General Leonel e ao general Carvalho.

Senhores, realmente reforço minhas palavras iniciais da satisfação em estar nesta tarde fazendo a abertura do Ciclo de Estudos Estratégicos. Sempre quando retornamos a esta casa, nos sentimos realmente estimulados, pois se trata de um local onde pensa o futuro do Exército Brasileiro, onde se reúnem pessoas do mais alto nível no que se refere ao senso crítico, onde é possível a realização de um Ciclo de Estudos Estratégicos sobre um tema tão relevante para nós. Não teria lugar melhor para acontecer do que aqui. Permitam-me os militares que eu vou falar um pouquinho do Órgão que eu tenho prazer em estar à frente.

O Comando de Operações Terrestres (COTER) é o órgão de mais alto nível do Exército Brasileiro voltado para o preparo e para o emprego da Força. Preparo significa identificar quais são as hipóteses de emprego do Exército Brasileiro, quer seja na guerra de alta intensidade e convencional, quer seja na guerra de mais baixa intensidade, situada na outra ponta do espectro.

Por exemplo, por ocasião da realização da Operação Pipa, nós identificamos todas as hipóteses de emprego da Força e traçamos um roteiro a ser seguido. Por intermédio do Centro de Doutrina, o COTER orienta o preparo que uma Força precisa receber para fazer frente a este tipo de missão. Em suma, como uma Força deve se equipar, quais são os equipamentos necessários e como a tropa deve ser treinada. No que se refere ao emprego, entende-se que são as operações propriamente ditas. Ou seja, nós orientamos o emprego dizendo quais Forças serão empregadas, adjudicando meios e pessoal necessários para que estas Forças possam cumprir suas missões.

* Comandante de Operações Terrestres do Exército Brasileiro.

Identificamos que uma das propostas deste ciclo é compreender que o ambiente cibernético é a nova dimensão do campo de batalha. Neste sentido, nota-se que o tema em pauta tem tudo a ver com o COTER e com a doutrina, porém não é um assunto fácil para o COTER, tendo em vista que é um tema relativamente novo até em termos mundiais. Praticamente não há uma doutrina estabelecida nos países. Haja vista seu aspecto sigiloso fica um pouco difícil nós conversarmos sobre esse assunto. Sendo assim, a nossa proposta nesta tarde é entendermos o ambiente cibernético como sendo a nova dimensão do campo de batalha e como as ações que produzem danos são conduzidas nesse ambiente operacional. Em torno disso, faremos a nossa apresentação de abertura deste Ciclo de Estudos Estratégicos. Tentaremos conversar sobre alguns conceitos que podem criar cenários, que certamente servirão de base para estimular os debates ao longo dos próximos dois ou três dias.

2. Desenvolvimento

Apresentaremos alguns conceitos, teremos alguns casos reais de utilização do *ciberespaço* para realização de ataques, destacando que já há casos de ação em força no *ciberespaço*, estabeleceremos um cenário típico de um ataque cibernético e partiremos para a nossa conclusão.

Vou falar um pouquinho de doutrina. Nós temos o nosso manual de operações, que é elaborado pelo Centro de Doutrina do Exército:

Figura 1 - A doutrina do Exército Brasileiro

Fonte: o autor, 2019.

Na sua edição de 2017, trabalhamos com três dimensões operacionais: a dimensão humana, a dimensão física e a dimensão informacional. Lembro que os militares, culturalmente, trabalhavam muito com as duas primeiras dimensões: humana e física. A

partir de 2017 nós entramos com a dimensão informacional, modificando o conceito de ambiente operacional, que passa a ser compreendido como o conjunto de condições e circunstâncias que afetam o espaço onde atuam as Forças Militares, bem como interfere na forma como são empregadas as respectivas Forças Militares.

Dito isto, passo a discorrer sobre o conjunto de condições e circunstâncias que afetam o espaço onde atuam as Forças Militares. Não defini como domínio, porque nós veremos que não temos ainda o *ciberespaço* como sendo um único campo. Este termo ainda não é, em termos doutrinários, uma dimensão específica e por isso não separamos o *ciberespaço*, da dimensão informacional. Agimos dessa forma porque não aceitaremos a doutrina americana, haja vista que a mesma compreende o *ciberespaço* como sendo um domínio.

Conforme a figura abaixo, a dimensão informacional abrange os sistemas utilizados para obter, produzir e atuar sobre a informação:

Figura 2 - As dimensões/domínios do campo de batalha

Fonte: o autor, 2019.

Quando esse conceito foi estabelecido, tínhamos a pretensão de reforçar a importância da guerra das percepções, da informação, da obtenção da superioridade da informação e da conquista da narrativa. O ambiente informacional trata desse assunto e coloca os sistemas utilizados para obter e produzir informação, como sendo uma mera ferramenta para a obtenção da superioridade informacional. O ambiente do *ciberespaço* ainda está em construção.

Por outro lado, quando nós lemos o manual de operações dos Estados Unidos da América de 2017, constatamos a utilização do conceito de domínio dando um

entendimento de que a guerra é travada em cinco domínios: terra, ar, mar, espacial e *ciberespaço*:

Figura 3 - A doutrina norte-americana

Fonte: o autor, 2019.

Terra, ar e mar já são domínios consagrados para os militares. No domínio espacial, verifica-se que poucos países possuem a capacidade de conduzir e dominar este domínio. Parece redundância, mas dominar este domínio é algo complexo que indica, em termos militares, o total controle de todos os processos: desde a aquisição de um satélite geoestacionário na órbita terrestre, até os operadores de informação. Dessa feita, informo que o Brasil não domina este ambiente operacional, pelo simples fato de não ter o controle de todos os processos.

Passando para o *ciberespaço*, verifica-se que os Estados Unidos da América (EUA) definem *ciberespaço* como sendo um dos cinco domínios operacionais e que permeia todos os demais: terrestre, marítimo, aéreo e espacial. O domínio da *internet* pode criar a liberdade de ação para realizar atividades em outros domínios. De acordo com o manual norte-americano, *ciberespaço* é um espaço virtual composto por dispositivos computacionais conectados em rede ou não, onde as informações digitais transitam, são processadas e armazenadas.

Vejam a similaridade com o nosso conceito de ambiente informacional. A diferença é que o ambiente informacional está voltado para a obtenção da superioridade da informação, ao passo que a definição norte-americana visualiza como sendo um ambiente operacional, que visa ser um ambiente propício para a condução de ações em força por parte dos Estados.

Então senhores, estamos trabalhando em conceitos. A pergunta que se faz é se nós estamos no campo das idéias ou se isto já é uma realidade? Então, vou responder: sejam bem vindos à realidade.

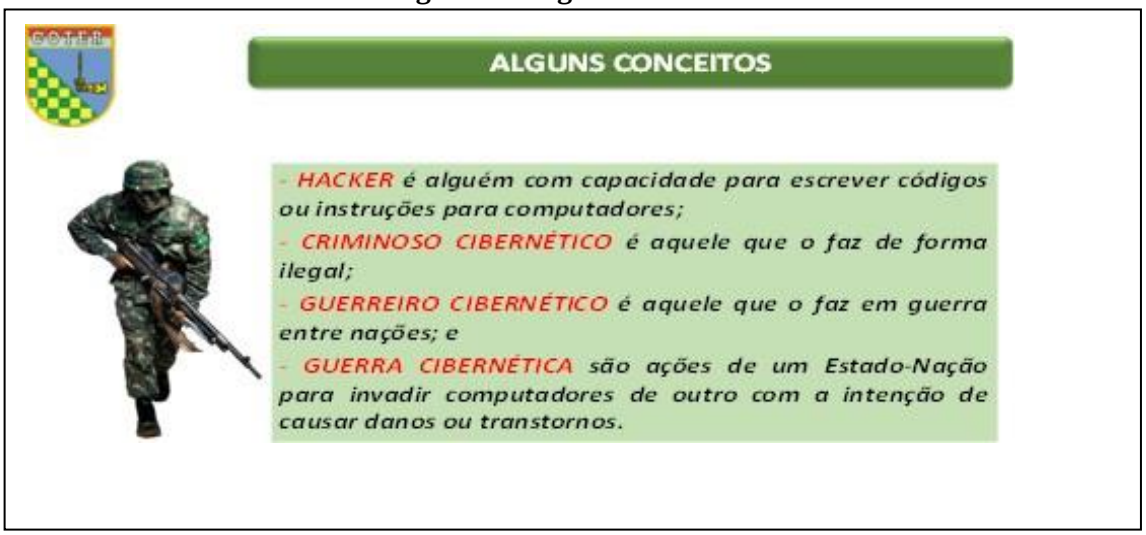
Figura 4 - Campo das ideias ou realidade

Fonte: o autor, 2019.

O ambiente cibernético está presente no nosso dia a dia. Nós não sabemos, mas quando nos debruçamos numa pesquisa e reunimos as informações, percebemos o quanto nós somos dependentes. Essa dependência, de certa forma, até nos assusta por conta das possibilidades dos danos que podem ser causados por conta dessa dependência.

Discorro a seguir sobre alguns conceitos para que nós possamos conversar de maneira bem clara:

Figura 5 - Alguns conceitos



Fonte: o autor, 2019.

Hacker é alguém com capacidade para escrever códigos ou instruções para computadores, pelo que também é um assunto bem atual. Temos visto nas últimas duas

semanas o que pode ser feito nessa área por um criminoso cibernético (*hacker*), que faz essas ações de forma ilegal.

Já o conceito de guerreiro cibernético, entende-se que é aquele que atua no contexto de uma guerra entre nações. No que se refere à guerra cibernética, verifica-se que são ações de um Estado-Nação contra o outro, no intuito de invadir computadores com a intenção de causar danos ou transtornos.

Vamos ver alguns casos reais. De antemão colocamos apenas o que está na literatura. Conforme foi dito anteriormente, a maioria dos países nega a ocorrência desses fatos. Assim, compilamos e trouxemos aqui somente o que está presente na literatura para que os senhores tenham uma idéia do que está acontecendo no mundo.

O primeiro exemplo remonta ao ano de 2003. Nesse ano, os Estados Unidos da América (EUA) penetraram na rede do Ministério da Defesa iraquiano às vésperas de sua invasão no Iraque. Apoderaram-se de endereços de *emails* de militares iraquianos e enviaram *emails* para os mesmos desestimulando-os a praticar resistência, orientando-os a abandonarem a posição. Foi uma operação psicológica que se apoiou de uma operação cibernética. Surtiu efeito, pois reduziram de forma considerável as resistências iraquianas.

Outro exemplo repousa no ataque perpretado pela força aérea israelense numa instalação nuclear síria em 2007. Nessa ocasião, os radares sírios foram infectados e não detectaram os aviões israelenses no espaço aéreo sírio. Enquanto os radares sírios mostravam o céu de brigadeiro, os aviões israelenses se aproximavam e atacavam as posições sírias sem serem molestados. Há várias hipóteses de como isso teria acontecido, desde hipóteses futuristas de que Israel tinha lançado um drone, que havia sido detectado pelos radares sírios, mas em contrapartida teria devolvido um sinal que continha um vírus capaz de infectar os radares sírios, ou até de espiões israelenses que inseriram um *malware* na linha de defesa síria.

Outro caso é o ataque russo à Estônia em 2007. Na verdade, tratou-se de um ataque de negação de serviço à Estônia, que é considerada um dos países mais conectados do mundo. Tal ataque afetou os sistemas bancários, os sistemas de comunicações, comércio e outros, fazendo com que esses sistemas ficassem indisponíveis por vários dias. Foi um ataque muito bem conduzido. Num determinado momento, o ataque era direcionado ao sistema bancário, afetando e inviabilizando todo sistema bancário. Quando a Estônia começava a restabelecer o sistema bancário, o ataque era redirecionado para outro sistema. Em síntese, esses ataques tiraram a população da Estônia da sua tranquilidade e da normalidade do seu padrão de vida por vários dias.

No ano de 2008, por ocasião da invasão russa na Geórgia, os russos desencadearam ataques de negação de serviço de C². Tal ataque foi direcionado aos sistemas de comunicações do país e tinha o objetivo de degradar os sistemas de comando e controle da Força Terrestre da Geórgia, aspecto que dificultou a reação da Geórgia face a investida russa. A população não sabia o que estava acontecendo. Não sabia se o país estava sendo invadido, da mesma forma que o mundo afora também não sabia o que estava acontecendo na Geórgia.

Outro fato ocorreu em 2009, por ocasião da realização de um exercício de defesa cibernética combinado, realizado entre os EUA e a Coréia do Sul. Dessa forma, a Coréia do Norte resolveu fazer um ataque de negação de serviços contra *sites* dos EUA e da Coréia do Sul, tirando do ar vários sites de diversas empresas internacionais. Da mesma forma como ocorreu na Estônia, tais ataques também foram muito bem organizados e conduzidos. Num determinado momento, os ataques eram direcionados aos sites do governo norte-americano, em outro momento os ataques eram redirecionados para empresas e para o governo da Coréia do Sul e assim foi se sucedendo.

Outro exemplo repousa num ataque conduzido contra o Irã em 2010, o qual ficou conhecido por *Stuxnet*. EUA e Israel produziram um sofisticado vírus que atacou a usina de enriquecimento de urânio de Natanz, no Irã, causando leves danos físicos às cascatas de centrífugas, fato que atrasou o projeto nuclear iraniano por vários anos. Foi um ataque cibernético com efeito cinético.

Outro exemplo de ataque cibernético e conhecido por todos, foi a interferência russa na campanha presidencial norte-americana em 2016. Em síntese, o ataque foi uma campanha cibernética compondo de uma operação psicológica para atuar contra a campanha da então candidata à presidência dos EUA: *Hillary Clinton*.

Em 2019 registra-se nova ocorrência de um ataque cibernético. Dessa vez, envolvendo Israel e o grupo fundamentalista *Hamas*. Em linhas gerais, as Forças Armadas israelenses descobriram o local que abrigava o comando cibernético do grupo *Hamas* e bombardearam o respectivo local, causando severos danos às ações do *Hamas* no ambiente *web*. Foi um ataque cinético, com efeitos cibernéticos.

Em 23 de junho de 2019, os senhores devem ter ouvido falar ou terem lido que o Irã abateu um drone norte-americano. Como consequência, os EUA teriam lançado mais um *ciberataque* ao Irã. Os norte-americanos ainda não sabem quais foram as consequências e os danos decorrentes dessa investida.

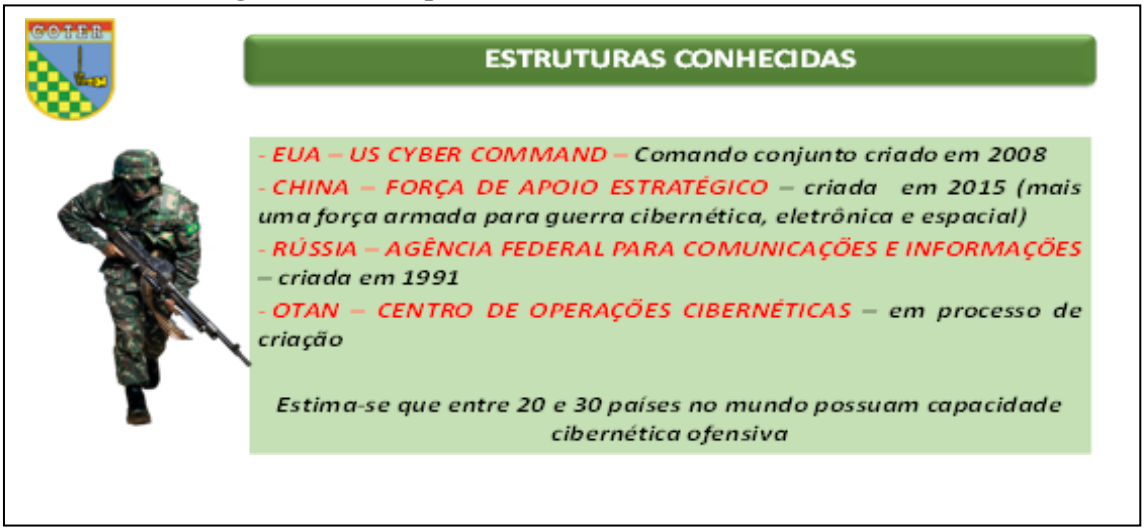
Figura 6 - Ataque cibernético norte-americano contra o Irã

Fonte: o autor, 2019.

Como foi dito anteriormente, na maioria dos casos os governos negam o envolvimento e quando são identificados ataques vindos de seus territórios, os mesmos respondem que são pessoas e não o Estado. Em alguns casos, pôde-se comprovar o vínculo que havia entre os *hackers* e as organizações governamentais. Inclusive, agumas organizações de máfia poderiam estar vinculadas a determinados governos.

Há várias estruturas que tratam desse assunto nos EUA. Na China, há uma Força de Apoio Estratégico. A Rússia possui a Agência Federal para Comunicações e a OTAN está criando o seu Centro de Operações Cibernéticas. Além disso, nota-se que os EUA, a Rússia, a França e Israel estão criando unidades militares especializadas em guerra cibernética. Com exceção da OTAN, percebe-se que as unidades de guerra cibernética estão sendo criadas dentro de grandes Unidades Militares:

Figura 7 - Principais estruturas cibernéticas no mundo



Fonte: o autor, 2019.

Estima-se que cerca de trinta países no mundo possuem capacidade cibernética ofensiva, ou seja, podem conduzir uma ação em força nesse ambiente que foi o objeto de estudo hoje à tarde: *ciberespaço*. Quais são os países que estão na ponta desse processo? Respondo dizendo que Estados Unidos, Rússia, França, Israel, as duas Coreias e China são os países mais avançados e podem causar algum estrago na condução desse tipo de operação.

De toda sorte, verifica-se que esse tipo de operação pode ser conduzida em qualquer parte. Basta existir uma pessoa, um computador, um processador, um cabo conectado na rede, não somente a *internet* (que é a maior rede aberta do mundo), ela inclui a *internet* e outras redes que deveriam estar isoladas da *internet*, mas não estão. Uma vez conectados à internet, nós temos uma vulnerabilidade. É possível chegarmos a uma loja de alta tecnologia e vermos alguns anúncios em alguns países que a máquina de lavar roupa, o fogão e o elevador podem ser controlados pelo fabricante, via *internet*. Ou seja, se tem IP, é possível atacar até a máquina de lavar louças da sua casa tirando-a de funcionamento, não respeitando as fronteiras físico-geopolíticas. Em síntese, as operações podem acontecer em qualquer lugar e podem ser deflagradas em locais fisicamente afastados, aspecto que coloca em xeque nossas defesas tradicionais.

Temos uma Força Terrestre potente, mas isto por si só, não assegura a defesa contra um ataque cibernético. Diferentemente de outras armas, seus alvos mais comuns são civis, principalmente as estruturas críticas. E este é um grande problema para os países desenvolvidos, que possuem programas computacionais em toda sua rede de infraestrutura civil. Esses programas normalmente atendem aos órgãos de Estado e aos Departamentos de Defesa, ou seja, há uma grande vulnerabilidade nessa infraestrutura civil que presta o serviço do dia a dia para a sociedade. Lá é onde a sociedade percebe a sua vida rotineira, a sua vida tranquila. Sem causar alardes, a guerra cibernética atua de forma diferente, pois tudo é revestido de sigilo.

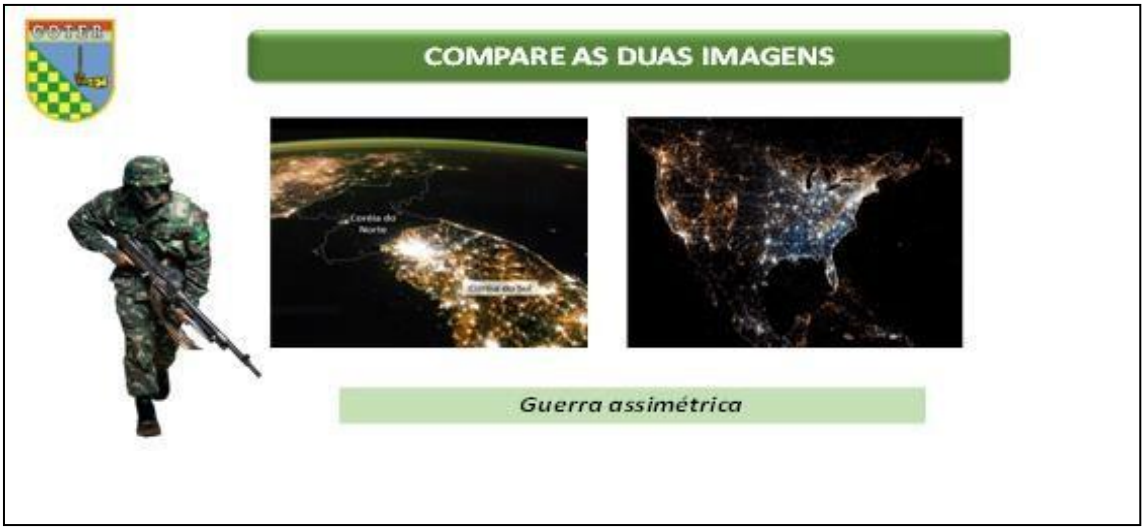
Não há dissuasão na guerra cibernética. Isso favorece o desencadeamento de ações voltadas para a necessidade de defesa da estrutura de governo: incluindo o setor de defesa e a estrutura corporativa civil. Em suma, quanto mais desenvolvido for o país, maior será a sua dependência do *ciberespaço* e conseqüentemente, sua vulnerabilidade.

Poucas pessoas, com meios relativamente escassos, podem gerar um efeito destruidor significativo. Há dificuldade para compreender a origem dos ataques, uma vez que dificilmente os elementos são identificados e raramente conseguem detectar quais

são os países que estão por detrás disso. Diante dessas considerações, nota-se que há necessidade de ter o controle no mais alto nível.

Vejam os senhores, por exemplo, a Coreia do Sul e a Coreia do Norte. Veja o potencial de danos que a Coreia do Norte, que sabemos que é um protagonista neste ambiente, pode causar na Coreia do Sul. Observem a figura abaixo:

Figura 8 - Guerra Assimétrica



Fonte: o autor, 2019.

Vamos imaginar alguns cenários possíveis em um ambiente de guerra cibernética. O primeiro cenário é um ataque ao sistema financeiro, onde seja possível apagar todos os meios eletrônicos. Imagine o caos que isso iria trazer a um determinado país nos dias atuais. Hoje tudo é virtual. Quase todas as nossas operações bancárias são desencadeadas no ambiente cibernético. Não seria terrível se o nosso saldo sumisse do banco do dia para noite e perdessem todas as referências? É dessa forma que o caos iria se estabelecer num determinado país.

O segundo cenário seria um ataque ao sistema de telecomunicações, pelo que fatalmente iria isolar as comunicações. Na Geórgia, vimos que houve 70% da perda do total de comunicações, fato que tornou vulnerável o país.

O terceiro cenário recai num ataque ao sistema de transportes. O sistema de transportes aéreo é altamente dependente das comunicações. Um controlador aéreo não consegue ver onde estão seus aviões. O piloto lá em cima não sabe qual altitude encontra sua aeronave. Esses aspectos certamente iriam provocar um acidente aéreo. ou até mesmo uma queda de aviões.

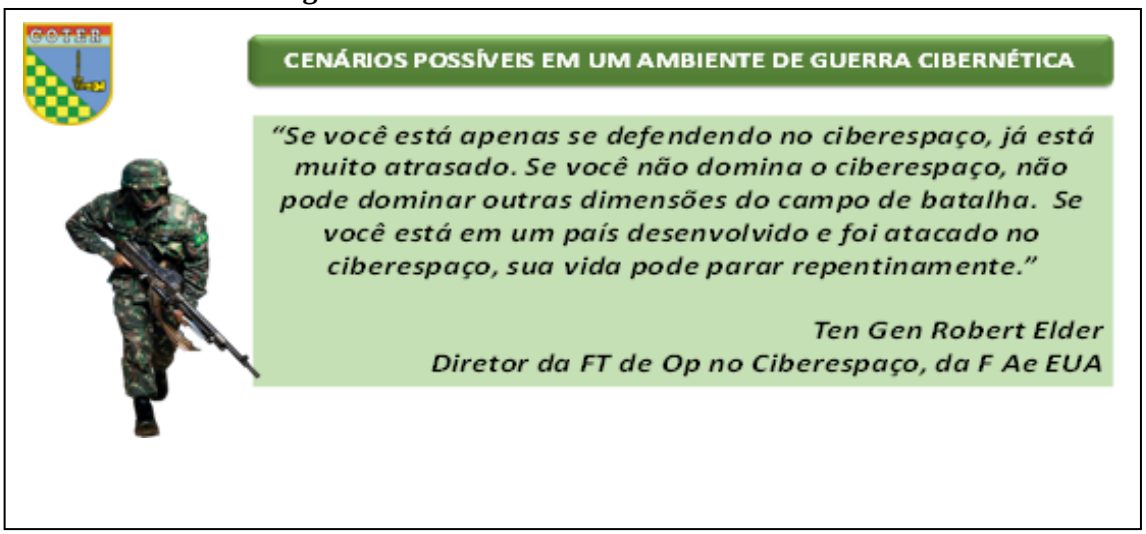
O quarto cenário é um ataque a infraestruturas críticas. Dizem que atualmente a Venezuela estaria sendo alvo de alguns ataques cibernéticos destinados ao sistema elétrico e a determinadas refinarias. Para causar explosões em refinarias, basta alterar o

funcionamento das usinas nucleares, modificar as condições de segurança de um reator nuclear e teremos um problema nuclear enorme. No que concerne às hidrelétricas, basta alterar a rotação das turbinas, aspecto que taticamente inviabiliza o funcionamento da mesma. Então, não se trata de um cenário de filme de ficção. Todos esses cenários são possíveis de acontecer nos dias atuais. Basta um ataque cibernético ser realizado segundo uma dessas situações.

Na área militar, há possibilidade de nós degradarmos o ambiente informacional, para que as Forças Convencionais tenham mais liberdade de ação naqueles três domínios: no ar, no mar e na terra. Ou para que tenhamos mais liberdade de ação nas dimensões que nós trabalhamos, degradando o sistema de comando e controle, favorecendo as operações de desativação e engano de radares, sensores, bem como favorecendo a desativação de armas e como instrumento de operações psicológicas.

Um general americano emitiu a seguinte frase acerca do ambiente cibernético no início deste século:

Figura 9 - Ambiente cibernético no ano 2000



Fonte: o autor, 2019.

Como disse às vezes, uma Força Terrestre muito forte pode não ser o suficiente para fazer frente a um ataque cibernético. Se você está em um país desenvolvido e se o mesmo for atacado no *ciberespaço*, sua vida pode parar repentinamente.

E como é que nós tratamos isto no Brasil? A nossa Estratégia Nacional de Defesa levantou quais são os três assuntos de maior relevância a serem tratados pelas Forças, nos projetos em curso: 1) o setor nuclear foi atribuído à Marinha do Brasil; 2) o setor espacial foi atribuído à Força Aérea Brasileira; e 3) o setor cibernético foi atribuído ao Exército Brasileiro.

No que se refere ao setor cibernético, o Brasil trabalha com estas esferas de responsabilidade de acordo com a figura abaixo:

Figura 10 - Esferas de responsabilidade no setor cibernético brasileiro

Fonte: o autor, 2019.

O nível político comanda todo o setor cibernético e está representado pela presidência da república. O segundo nível é o estratégico e está representado pelo Ministério da Defesa, Estado Maior Conjunto das Forças Armadas e as Forças Armadas. O terceiro nível é o operacional e se faz representado pelo Comando de Operações do Comando Conjunto. No nível tático, a responsabilidade pela condução da guerra cibernética recai sobre as Forças Componentes, mais precisamente na Força Conjunto de Guerra Cibernética.

É dessa forma que estamos estruturados no país: dois níveis conduzem a guerra cibernética: ataque a nível de operações (nível operacional e nível tático) e a defesa cibernética no nível estratégico (nível Ministério da Defesa). Lembrando a importância do conversível, um Comando Conjunto no nível político (responsabilidade da presidência da república).

3. Conclusões

A guerra cibernética é real e o que está acontecendo é uma amostra do que pode acontecer em larga escala. Os contendores não mostraram todo o arsenal. Esses ataques identificados em princípio são somente uma pequena amostra do que os mesmos são capazes de fazer. Às vezes, até testam os sistemas de defesa adversários. Nós não sabemos qual é o verdadeiro potencial de quem está atacando.

A guerra cibernética é global e a interconectividade mundial transforma um ataque, num assunto de interesse mundial. A guerra cibernética para alguns especialistas

já começou. Esses ataques são apenas um teste para os sistemas: ataque contra defesa, *ciberespaço* e o campo de batalha.

Dessa forma, encerro a minha participação. Não espero que essas informações que nós trouxemos aqui esgotem o assunto. Na realidade, vocês viram que nós compilamos inúmeras informações para fazer a ambientação para o início do Ciclo de Estudos Estratégicos e tenho certeza de que pode ser útil aos senhores na evolução do trabalho. Volto a falar da imensa satisfação que eu tenho de estar diante dos senhores aqui. Aguardamos o resultado desse Ciclo de Estudos Estratégicos. Certamente será um produto muito útil para nossa doutrina.

Obrigado a todos pela atenção!

A COMUNICAÇÃO ESTRATÉGICA DO EXÉRCITO E A DIMENSÃO INFORMACIONAL

General de Divisão Richard Fernandez Nunes*

1. Introdução

A comunicação estratégica[1] pode ser definida como a comunicação integrada, sincronizada e alinhada com as ações realizadas por uma organização para atingir seus objetivos. Pressupõe a combinação das práticas adotadas no âmbito da comunicação social tradicional (BRASIL, 2017) com relações institucionais sistematizadas e com o emprego das mídias digitais, aí incluídas as mídias e as redes sociais. Tal conceito de comunicação, típica do meio corporativo, é perfeitamente aplicável à comunicação no âmbito do Exército Brasileiro (EB).

O propósito deste trabalho é analisar o desenvolvimento da comunicação estratégica do EB em meio à complexidade que caracteriza a dimensão informacional, extrapolando ambos os conceitos de modo a serem aplicados tanto na vertente institucional quanto no âmbito operativo dessa comunicação, considerando-se a crescente relevância das ações realizadas no espaço cibernético.

A doutrina militar terrestre preconiza que o ambiente operacional onde se desenrolam as ações militares compreende três dimensões: 1) a física, de natureza geográfica e material, com ênfase para o terreno, as condições meteorológicas e os equipamentos empregados; 2) a humana, de caráter psicossocial e cultural, pautada pelas interações entre as tropas e populações envolvidas; e 3) a informacional, altamente dependente de meios tecnológicos, centrada na elaboração de narrativas que retratem a percepção da realidade (BRASIL, 2017b).

Sobre esta configuração, paira o espaço cibernético apresentado na figura a seguir, no qual se observa a aceleração, a potencialização e a automação dos mais diversos sistemas e processos, sem perder de vista a intencionalidade humana no fenômeno da comunicação.

---

* Chefe do Centro de Comunicação Social do Exército.

[1] Não há definição consolidada na literatura acerca desse conceito. Entretanto, há consenso de que se trata de ações integradas de comunicação com vistas à conquista dos objetivos organizacionais.

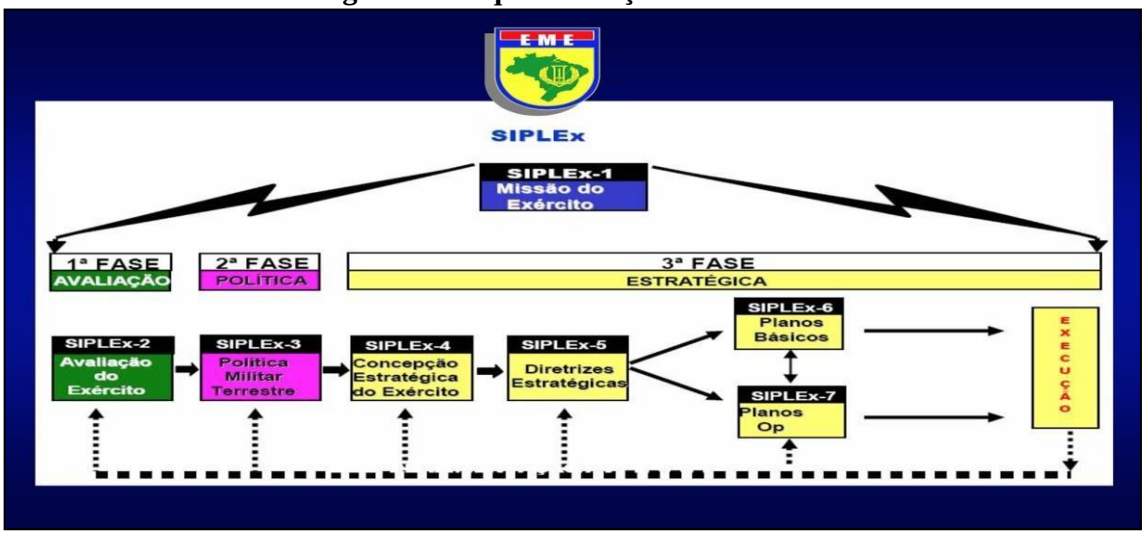
Figura 1 - Dimensões do ambiente operacional

Fonte: BRASIL, 2017b.

2. A Comunicação no Exército Brasileiro

O Exército Brasileiro explicita, por meio de seu Sistema de Planejamento Estratégico (SIPLEx), os objetivos a serem alcançados pela instituição, bem como detalha as condições de realização das ações planejadas, conforme a figura abaixo:

Figura 2 - Esquematização do SIPLEx



Fonte: SIPLEx, 2005.

Alinhada com o SIPLEx, a comunicação do EB adquire feição estratégica, a ser ratificada conforme a capacidade de integração e sincronização que for capaz de obter, seja em relação aos objetivos específicos que lhe competem, seja no apoio à consecução dos demais.

O sistema corporativo encarregado da comunicação social do Exército é o SISCOMSEx[2], cujo órgão central é o Centro de Comunicação Social do Exército (CCOMSEx), a quem compete propor os planos e diretrizes, bem como coordenar as ações correspondentes, valendo-se de rede dedicada a esse fim: a RESISCOMSEx[3]. Além dessa atribuição, o CCOMSEx tem sua atuação na vertente institucional ampliada pela missão de ser um dos órgãos de assistência direta e imediata (OADI) ao Comandante do Exército Brasileiro.

O caráter estratégico, eminentemente institucional, permanente e sistemático da comunicação social do Exército Brasileiro não restringe, ao contrário, potencializa sua participação no ambiente operacional, particularmente no âmbito das operações de informação, como sendo uma das capacidades relacionadas à informação (BRASIL, 2014). Neste caso, **a comunicação estratégica assume feição operativa**, como ferramenta indispensável para multiplicar o poder de combate, fortalecer o espírito de corpo e o moral da tropa, na **dimensão humana**; bem como para buscar o domínio da narrativa a fim de se obter o apoio da opinião pública, centro de gravidade da **dimensão informacional**.

Em qualquer situação, considerações acerca das atividades no *ciberespaço* se impõem devido aos relativos baixos custos que requerem e à dificuldade de se atribuir responsabilidades de narrativa nesse meio, tão propício à ambiguidade.

Considerando essa gama de responsabilidades, cabe ao CCOMSEx **a missão precípua de preservar e fortalecer a imagem do Exército Brasileiro,** condição essencial para que a instituição atinja seus objetivos que, ao longo de sua trajetória histórica, tem desfrutado de ilibada reputação e dos mais altos índices de credibilidade junto à sociedade brasileira.

3. A Preservação da imagem do Exército Brasileiro

A missão de preservar a imagem do Exército Brasileiro subentende abordagem preventiva e reativa, diante das ameaças potenciais ou concretas que possam afetá-la. Os ativos mais relevantes a se proteger são exatamente os elementos essenciais da reputação e da credibilidade desfrutadas pela instituição. Assim, os princípios éticos e os valores

[2] Sistema composto por agências classe A, B, C e Especiais, estruturas de comunicação social distribuídas por todas as organizações militares do Exército (BRASIL, 2017b).
[3] Rede colaborativa pela qual os integrantes do sistema estabelecem as ligações do canal técnico necessárias ao funcionamento do SISCOMSEx (BRASIL, 2017b).

morais que a sustentam, a cultura organizacional que a caracteriza e a narrativa consolidada de sua trajetória histórica, precisam ser permanentemente protegidos contra posicionamentos adversos que, de modo explícito ou dissimulado, possam atingir a imagem da Força e dificultar a consecução de seus objetivos estratégicos.

Nesse contexto, devem ser objeto de redobrada atenção: os estabelecimentos de ensino do EB e a educação militar por eles proporcionada, reconhecida pela qualidade e pelo culto aos valores centrais da instituição; a memória aos patronos e a outros fatos históricos em que a Força Terrestre se notabilizou; a honorabilidade dos comandantes, chefes e diretores em todos os níveis; o respeito aos preceitos da hierarquia e da disciplina; o emprego atual da Força no amplo espectro das operações; bem como as narrativas elaboradas pela Força e difundidas pelo SISCOMSEx.

Eventuais deficiências observadas no tratamento desses temas podem se converter em vulnerabilidades passíveis de exploração negativa, com reflexos ainda mais expressivos se esta vier a ocorrer no espaço cibernético. A metodologia aplicada na análise de riscos à segurança orgânica é pertinente também nesta área. A exposição inadequada ou a superexposição de assuntos de interesse constituem riscos ponderáveis a considerar. A falta de alinhamento, de sincronização e de integração da comunicação, ou seja, a perda do seu caráter estratégico constitui o pior cenário, capaz de caracterizar fragilidade na segurança cibernética social. Tal segurança está relacionada ao entendimento e nas mudanças influenciadas pela cibernética no comportamento humano e seus resultados sociais, culturais e políticos (BESKOW; CARLEY, 2019).

As ameaças à imagem do Exército Brasileiro, como quaisquer outras que visem obstar a conquista de seus objetivos estratégicos ou operacionais, podem ser de origem interna ou externa, provenientes de forças oponentes regulares, de forças oponentes irregulares, de organizações não governamentais (ONG's), de agências diversas, de produtores de mídia e de atores não estruturados. Os ataques que podem ser desferidos na dimensão informacional visam, em última análise, a contraposição de narrativas alternativas, com ou sem fundamento nos fatos, as chamadas *fake news*. Nesse cenário, são comuns o emprego de *hackers, bots e trolls*[4], para manipular, distorcer, descontextualizar e falsificar perfis e conteúdos relacionados à instituição.

[4] Típicos atuadores no *ciberespaço*, *hackers* são indivíduos capazes de produzir modificações não autorizadas em sistemas computacionais. *Bots* são *softwares* desenvolvidos para atuar como robôs simulando ações humanas. *Trolls* são agentes perturbadores da edição de conteúdos e das discussões nas redes sociais.

A resposta adequada à concretização dessas ameaças depende de efetivo monitoramento do espaço cibernético com ferramentas tecnológicas desenvolvidas para analisar tudo o que circula em meio digital e que possa estar relacionado aos interesses do Exército Brasileiro. Nessa tarefa, a comunicação estratégica, a inteligência e a defesa cibernética precisam atuar absolutamente integradas, de modo a proporcionarem acurado assessoramento à tomada de decisão, daí decorrendo as ações diretas e indiretas a serem realizadas. Para o êxito da missão de preservação da imagem da Força, iniciativa e liderança são atributos fundamentais a serem observados em todos os níveis. Com a velocidade e a abrangência que caracterizam as ações no espaço cibernético, não há tempo a perder para a adoção oportuna das medidas preventivas ou reativas que se fizerem necessárias.

4. O fortalecimento da imagem do Exército Brasileiro

A missão de fortalecer a imagem do Exército Brasileiro tem enfoque proativo, com vistas ao aproveitamento de todas as oportunidades oferecidas ou criadas para a veiculação de mensagens favoráveis, por todos os integrantes do SISCOMSEx. A conquista do apoio da opinião pública confere a legitimidade necessária à obtenção de liberdade de ação para a consecução dos objetivos estratégicos e operacionais da Força.

A legitimidade também está relacionada à compreensão da importância estrutural do Exército Brasileiro na sociedade. Neste âmbito, a academia proporciona a validação e a credibilidade necessárias para a construção do discurso que é disseminado por diferentes meios de comunicação, entre eles o periódico científico. A comunicação científica validada pelos pares, avaliada e reavaliada constantemente, transfere credibilidade e legitimação do trabalho realizado pelo Exército Brasileiro em conjunto com a sociedade, que participa diretamente dessa construção.

A atitude mais positiva é a difusão e o reforço de narrativas, de modo integrado e sincronizado, acerca dos elementos essenciais da reputação e da credibilidade da instituição, considerando-se que "tudo comunica!". Neste sentido, todos os veículos disponíveis devem ser mobilizados, com especial atenção para as plataformas digitais. A busca de parcerias com órgãos externos à Força capazes de multiplicar o efeito dessas narrativas é altamente recomendável. Para isso, a sistematização das relações institucionais, inclusive com órgãos de mídia, constitui componente relevante da comunicação estratégica do Exército Brasileiro.

O emprego alinhado, integrado e sincronizado das mídias digitais no âmbito do SISCOMSEx é impositivo para o êxito na missão. Para isso, foram publicadas as Normas para Criação e Gerenciamento das Mídias Sociais no Âmbito do Exército Brasileiro em 1º de julho de 2019 (BRASIL, 2019). Tais normas constituem instrumento disciplinador essencial para a comunicação estratégica do Exército Brasileiro, deixando claro o que é permitido e desejável, sempre resguardando a instituição de eventuais interações prejudiciais às narrativas da Força.

O fortalecimento da imagem do Exército Brasileiro comporta também o emprego de inteligência artificial. Em 1º de março de 2019, foi "incorporado às fileiras do Exército" o Soldado MAX, cujo nome é uma abreviatura de Módulo Auxiliar de relações públicas e uma homenagem ao herói brasileiro da 2ª Guerra Mundial[5]. Iniciativa inovadora, esse *chatbot* desenvolvido pelo Exército Brasileiro tem demonstrado excepcional capacidade de interação, particularmente com segmentos de público mais jovens interessados em ingressar na Força Terrestre.

No que concerne às dimensões do ambiente operacional, todas perpassadas pelo espaço cibernético, não se pode perder a noção de que a atuação de uma Força Armada está intrinsecamente ligada à geração de fatos reais, nas dimensões física e humana. A dimensão informacional remete a representações virtuais dessa realidade, as quais estão sujeitas a uma série de filtros de caráter multidisciplinar. A História, o Direito, a Sociologia, a Antropologia, a Psicologia, entre outras disciplinas, além de posicionamentos ideológicos diversos, condicionam a percepção da realidade. Sendo assim, a construção de narrativas direcionadas para o fortalecimento da imagem institucional do Exército Brasileiro, bem como da força empregada, precisa levar em consideração esse complexo espectro de áreas do conhecimento.

Um dos espaços adequados para a discussão e construção dessas narrativas nas diferentes áreas do conhecimento é o espaço acadêmico. Nele, a própria comunidade científica, livre e legitimada, desenvolve seus discursos. Para que isso ocorra, principalmente nas Ciências Sociais e Humanas, é preciso que haja diversidade de pensamentos, pesquisas e instituições, incluindo o Exército Brasileiro.

Na literatura que se tem produzido a respeito da chamada guerra híbrida, percebe-se a combinação dessas variáveis dimensionais, de modo integrado e sincronizado às

[5] Sargento Max Wolf Filho, morto em combate na região de Montese, na Itália, em 12 de abril de 1945.

tradicionais formas de combate, impactando o comportamento do público, muitas vezes com narrativas manipuladas no *ciberespaço* para a obtenção de legitimidade e da consequente liberdade de ação. O EB tem de estar preparado para esse tipo de conflito e nada mais adequado que adotar a proatividade para fortalecer a imagem e para dominar a narrativa, em tempos de paz ou de conflito armado.

5. Considerações finais

Como se pode depreender, a preservação e o fortalecimento da imagem do Exército Brasileiro, nos tempos atuais, indicam a necessidade de uma abordagem mais abrangente que a da comunicação social tradicional, de um redirecionamento para a adoção dos preceitos da comunicação estratégica.

Uma instituição com a reputação e a credibilidade do Exército Brasileiro deve boa parte dessa condição ao culto à verdade e à transparência, esta última salvaguardada pelo sigilo que envolve os temas de segurança nacional.

A chamada pós-verdade (POST-TRUTH, 2019), que opõe aos fatos o apelo a emoções, sentimentos, crenças e paixões ideológicas, a fim de se criar narrativas alternativas, tão em voga nos dias atuais, não se coaduna com a comunicação estratégica do Exército Brasileiro. Esse tipo de narrativa oportunista não perdura em sociedades democráticas e estruturadas em instituições sólidas. Não pode, entretanto, ser desprezado, devido aos danos que pode causar. A vitória, nesse contexto, demanda vigilância constante e permanente disposição para atuação proativa na dimensão informacional.

Com as possibilidades tecnológicas proporcionadas no espaço cibernético, acelerando, potencializando e automatizando ações informacionais, torna-se ainda mais relevante a observância de sólidos princípios éticos, garantia do caráter regular e permanente do Exército Brasileiro, condizente com a grandeza da missão de defender a Pátria Brasileira.

Referências

BESKOW, D. M.; CARLEY, K. M. Segurança cibernética social: um requisito emergente de segurança nacional. **Military Review,** Fort Leavenworth, KS, 3º Trim., p. 25-35, 2019. Disponível em: <https://www.armyupress.army.mil/Journals/Edicao-Brasileira/Arquivos/Terceiro-Trimestre-2019/Seguranca-Cibernetica-Social/>. Acesso em: 01 jun. 2019.

BRASIL. Exército Brasileiro. **Manual de campanha: operações.** 5ª ed. Brasília: Estado-Maior do Exército, 2017a. EB20-MF-03.103. Disponível em: <https://bit.ly/30ki plo>. Acesso em: 01 jun. 19.

BRASIL. Exército Brasileiro. **Manual de campanha: operações de informações.** Brasília: Estado-Maior do Exército, 2014. EB20-MC-10.213. Disponível em: <https://bit.ly/2KXwZCq>. Acesso em: 01 jun. 19.

BRASIL. Exército Brasileiro. **Manual de fundamentos: comunicação social.** 2ª ed. Brasília: Estado-Maior do Exército, 2017b. EB20-MF-03.103. Disponível em: <https://bit.ly/2Mnze5v>. Acesso em: 01 jun. 19.

BRASIL. Exército Brasileiro. **Portaria Nº 196-EME, de 1º de julho de 2019.** Aprova as Normas para Criação e Gerenciamento das Mídias Sociais no Âmbito do Exército Brasileiro. Brasília: EME, 2019. Disponível em: <https://bit.ly/2Z6e5n2>. Acesso em: 01 jun. 2019.

POST-TRUTH. *In:* **Lexico**. [S.l.]: Oxford, 2019. Disponível em: <https://www.lexico.com/en/definition/post-truth>. Acesso em: 01 jun. 2019.

SIPLEX. Sistema de Planejamento do Exército Brasileiro. SIMPÓSIO DE PESQUISA OPERACIONAL E LOGÍSTICA DA MARINHA, 2005. Rio de Janeiro. **Anais [...]** Rio de Janeiro: EGN, 2005. Disponível em: <https://bit.ly/2vAK4dR>. Acesso em: 01 jun. 2019.

SETOR ESTRATÉGICO CIBERNÉTICO

General de Divisão Guido Amin Naves*

1. Introdução

Senhor General Freitas, General Arruda e demais participantes anunciados anteriormente, é um prazer muito grande estar aqui na ECEME. Faço minha, as palavras do General Freitas em retornar à Escola de Comando e Estado-Maior do Exército. Para todos nós é sempre um momento de muita alegria e de renovação do espírito. Que a gente possa continuar enfrentando nossos desafios com mais motivação ainda.

Vocês podem imaginar como este oficial artilheiro, antiaéreo, então Chefe do Escritório de Projetos Estratégicos do Exército no EME se sentiu quando foi chamado numa tarde de outubro de 2017, na sala do Comandante do Exército Brasileiro. Nessa ocasião, fui informado pelo General Villas Boas, que no rodízio de março do próximo ano (2018), eu seria o Comandante Cibernético. Olhei bem para o Comandante do Exército e disse: General, onde é isso e o que eu tenho que fazer lá?

Falei isso porque era uma situação nova, difícil para mim. Afinal, sou artilheiro antiaéreo e estou habituado a lidar com radar e coisas do gênero. Imaginem como foi aquela minha primeira noite? Na verdade, foi uma noite tranquila porque a tranqüilidade dos ignorantes faz com que os mesmos durmam que nem um anjinho, mas foi a única noite que me permiti dormir.

Na verdade, esse é um assunto que precisamos, pois estamos sempre atrasados nesse assunto. Essa guerra acontece todos os dias e digo até com uma ponta de orgulho, que é o Comando mais operacional que eu servi na minha carreira.

Eu vou avançar e aprofundar em alguns conceitos. Com relação ao espectro de conflito, verifica-se que se trata de uma expressão já existente em nossa doutrina militar. A defesa cibernética opera 24 por 7, durante os 365 dias do ano. Não há um momento onde não exista um trabalho. Não pode se dar ao luxo de escolher onde e quando realizar uma ação cibernética. Desde o momento da paz até a parte mais escura do espectro, a atuação é diuturna. Não se pode deixar surpreender nesse espaço. A figura a seguir sintetiza essas informações:

---

* Comandante de Defesa Cibernética.

Figura 1 - Atuação da Defesa Cibernética

Fonte: o autor, 2019.

2. Desenvolvimento

O que a cibernética faz? Os postulados de *Sun Tzu* são perfeitamente aplicáveis no domínio informacional. A figura abaixo apresenta alguns conceitos importantes para o setor cibernético:

Figura 2 - Conceitos utilizados na cibernética

Fonte: o autor, 2019.

Primeiro, a cibernética não é intensiva em tecnologia, ela é dependente da tecnologia e o ambiente tecnológico é o nosso campo de batalha. A atuação nessa área requer conhecimento em conceitos bélicos e conceitos voltados à gestão administrativa.

A gestão administrativa precisa de rápida inovação. Eu comentei em um seminário de inovação na Folha de São Paulo, no final do ano passado, antes das eleições, que o problema maior nosso não era a tecnologia. Na verdade, a tecnologia é um eterno cabo-de-guerra que sempre busca atingir determinado ponto. A gestão administrativa não é

assim. O *ciberclock* é muito mais rápido, no minimo quatro vezes mais rápido que o *clock* normal de qualquer outra medição de tempo existente.

O nosso sistema de compras por exemplo. Eu não posso conceber uma compra simples na cibernética, como parafusos, arruelas, feijão ou arroz. O produto cibernético é muito complexo, pois necessita de longo tempo de investimento e quando chegar no produto final, o mesmo estará obsoleto. E aí, eu me deparo com a seguinte questão: o que eu faço com isso? Jogo fora porque mudou a era da cibernetica? A era cibernética muda a cada cinco anos e a mudança de uma era cibernética para outra é equivalente a mudança da idade média para idade moderna. Ou seja, torna-se necessário inovar na gestão e inovar na relação. Pessoal fala em dano ao erário, desvio de finalidade, etc. Mas, todo mundo fica receoso de querer dar um passo rumo ao desconhecido e isso atrasa tudo. E tudo na cibernética é rumo ao desconhecido.

Guardadas as proporções de nível de investimento e de estágio alcançado por cada país, nota-se que as discussões que envolvem o setor cibernético são exatamente as mesmas. Os Estados Unidos discutem muito como é que a defesa cibernética será incorporada no sistema de proteção elétrico, uma vez que ele é totalmente privado. No Brasil, o setor elétrico não é completamente privado, mas o setor de telecomunicações é todo privado. E como é que incorporo essas coisas no meu guarda-chuva estatal de proteção, uma vez que é importante proteger empresas como OI, CLARO, VIVO e TIM? Como eu faço isso? Elas são privadas, nós somos o Estado. São por essas razões que a inovação na gestão é importante, na medida em que alcança todos os setores.

A escalada é outro conceito importante na cibernética, tendo em vista que é muito fácil alguém atacar e o outro responder, replicar, treplicar e isso vai escalando. E aí acontece o que? Até onde eu vou com isso? Porque é muito fácil, não custa muito adotar essas ações. Se essas ações prosseguirem, eu posso escalar a crise a tal ponto de ocasionar uma paralisia estratégica em um determinado país. Será que é bom e interessante chegar nesse nível? Como é que uma sociedade vai reagir se chegar a esse nível de estresse? É por isso que o controle da escalada é muito importante, haja vista que é um conceito que vem desde a era nuclear, mas que agora nos obriga a uma nova leitura.

Lembra-se de quando se falava em destruição máxima assegurada e destruição total asegurada na era nuclear? Que um retalha, um atira e outro atira também, depois outro, outro e outro? No campo cibernético, isso ocorre com bastante frequência. Na cibernética é muito mais fácil e menos custoso chegar a um nível de fricção semelhante ao praticado entre norte-americanos e soviéticos.

Outro conceito é a assimetria. A cibernética é um grande redutor de assimetrias. Um exemplo disso é o grupo *Hamas*. O *Hamas* não é nenhum órgão estatal, mas se consiste numa organização que consegue causar grandes problemas para Israel por meio da ação cibernética do seu pessoal, que é altamente capacitado. Apareceu na internet um prédio em Israel onde servia de base para ações cibernéticas do *Hamas*, que foi explodido por tropas israelenses.

Outro conceito importante é atribuição. Por ser tão importante e atual, os Estados Unidos da América (EUA) vêm destinando elevada prioridade em pesquisas nessa área. A própria ONU reconheceu que uma ação cibernética proveniente do território de um país não é suficientemente capaz para atribuir a responsabilidade dos danos ao respectivo país. E isso é uma verdade. Basta olharmos para o nosso território, que é uma das maiores fontes de ataque ao território americano. Os norte-americanos, por sua vez, não nos retaliam porque eles têm consciência de que a autoria dos ataques não pode ser imputada ao Estado.

Eu posso ter um ataque de negação de serviço conduzido por geladeiras, televisões, máquina de lavar louças, qualquer equipamento. Já houve ataques aos agentes do Estado Brasileiro e quando foi investigado, descobriu-se que a origem provinha de um servidor situado na Finlândia. O Comando de Defesa Cibernético (ComDCiber) apenas informou o caso a Policia Federal e explicou que estava extrapolando a sua capacidade de ação.

Diante disso, surge a seguinte pergunta: Qual é o nível de certeza que preciso ter para poder retaliar um Estado? Está na imprensa que alguém conseguiu atribuir à Rússia a interferência nas eleições norte-americanas? Sabem o que o Chefe de Estado da Rússia disse? Ele respondeu relatando que foram *hackers* patrióticos e que não havia sido o Estado russo. E aí você faz o quê? Retalia assim mesmo? É difícil tomar uma decisão. Antigamente a atribuição era fácil. Em outros campos a atribuição também é fácil de fazer. O disparo de um míssil é de fácil atribuição, uma vez que você consegue ver a hora que ele saiu do chão. Agora, na cibernética não é tão simples assim. Torna-se necessária nova releitura sobre a atribuição.

Outro conceito é dissuasão. E como dissuade na *internet*? Na era nuclear era fácil, bastava ter um arsenal capaz de destruir até 427,5 vezes o oponente, que isso já gerava dissuasão. Na cibernética é diferente, uma vez que os países não difundem e nem tornam público as capacidades que possuem. Como a defesa cibernética requer a execução dessas três atitudes (proteção, exploração e ataque), geralmente os países não ficam alardeando

as suas capacidades. Por outro lado, quem recebe o ataque também não difunde qual foi o resultado, ocasionando mais incerteza ainda. No caso do *Stuxnet*, verifica-se que até hoje os Estados Unidos da América e Israel negam que fizeram o ataque ao Irã, que por sua vez, também nega que foi vítima desse ataque. A dissuasão no campo cibernético se materializa quando um determinado país tem interesse em mandar um recado a outro. E somente o destinatário vai entender o recado que foi dado. Dessa forma, nota-se que a dissuasão é outro conceito que precisa de uma releitura.

Outro conceito é o controle positivo de ações. Os norte-americanos entendem que esse conceito se traduz no controle sobre as ações cibernéticas que demandam intrusão não autorizada. Como é que um país vai entender uma intrusão não autorizada em seus sistemas por um determinado Estado? Ele pode entender isso como uma guerra. Nessa perspectiva, a própria estratégia americana propugna resposta cinética às ações cibernéticas tipificadas como intrusão. Ou seja, tem que estar em um nível elevado para poder tomar corretamente essa decisão. Vamos exemplificar: Se eu tenho uma tropa frente à outra tropa numa ação convencional qualquer e se essa tropa quiser atacar, entende-se que são ações no nível tático. Agora, uma instrusão no sistema de um Estado não é qualquer pessoa que pode autorizar o início de uma guerra.

Outro conceito é a paralisia estratégica. Esse conceito voltou. Ele tinha parado um pouquinho. Por exemplo, em meados do século XX você podia causar uma paralisia estratégica em um país com um ataque nuclear massivo. Atualmente, existem outras formas de causar paralisia estratégica. Nesse sentido, a literatura fala que foi exatamente isso o que a Rússia fez com a Estônia no ano de 2007.

O ataque russo infectou os sistemas da Estônia, deixando o país parado por dez dias, causando uma paralisia estratégica no país, uma vez que o mesmo possui o maior nível de governo eletrônico no mundo. Na Estônia, o cidadão só vai ao cartório para duas coisas: 1) casar e separar; e 2) comprar e vender imóvel. O restante das ações é realizado pelo sistema. O cidadão desse país só tem um documento: uma carteira de identidade com um *chip* e um número. Até no médico o cidadão vai com a carteira de identidade com *chip*. Imaginem esse país com ataque de negação de serviço, inviabilizando os seus sistemas por dez dias? Foi isso que ocorreu na Estônia, uma verdadeira paralisia estratégica. Esse é um conceito que volta pela facilidade de se conseguir a paralisia estratégica de um país usando o espaço cibernético.

Como é que a Defesa está organizada hoje para trabalhar na área cibernética? A figura a seguir elucida essa questão:

Figura 3 - A estrutura atual

Fonte: o autor, 2019.

O Comando Cibernético é um Comando Conjunto, cujo Chefe do Estado-Maior Conjunto é um Almirante da Marinha do Brasil. O Centro de Defesa Cibernética é o braço operacional, cujo chefe é um General de Brigada do Exército Brasileiro. O Departamento de Gestão Estratégica está sob o comando de um Brigadeiro da Força Aérea Brasileira. Há também a Escola Nacional de Defesa Cibernética (ENaDCiber), que foi ativada em fevereiro deste ano e está sendo comandada por um Coronel do EB.

Como o país trabalhou nisso? A figura a seguir sintetiza a evolução dos trabalhos desenvolvidos pelo país na área da Defesa Cibernética:

Figura 4 - A evolução da Defesa Cibernética

Fonte: o autor, 2019.

Os trabalhos se iniciaram em 2009, com o General Carvalho estando a frente do processo, tendo participado como Comandante. Nessa época, foram definidas as fases,

que se iniciaram, mas não acabaram ainda. Entre 2012 e 2016, o Brasil sediou uma série de grandes eventos. Nesse sentido, o país tinha que oferecer um nível adequado de proteção cibernética aos sistemas empregados nesses eventos, os quais passaram a ser prioritários no contexto da cibernética brasileira.

Mas, quando acabou o último grande evento, passou-se a questionar sobre os próximos passos que deveriam ser dados. Foram feitos estudos, diagnósticos, avaliações, etc. Ouvimos muita gente e concluímos que não podíamos esperar o término dessas fases de criação/implantação para iniciar uma consolidação, o que nos levou a mudar as prioridades elencadas. Por outro lado, verificou-se que era necessário buscar uma inserção política e estratégica do setor. Nós descobrimos que o nosso setor estava desequilibrado em relação aos demais, mesmo sendo tão importante quanto o nuclear e o espacial, até na questão de simples distribuição de recursos.

Estamos trabalhando no sentido de buscar a operatividade. Não buscamos ainda porque a demanda é muito grande. Nós temos que cuidar disso aqui agora para que esse setor seja utilizado para o Estado Brasileiro e para a sociedade brasileira, até porque são esses atores que irão nos demandar. Dessa forma, foi desenhado um modelo estratégico capaz de enquadrar todas as ações que teriam que ser feitas nos próximos anos no setor cibernético.

Figura 5 - Modelo Estratégico da Defesa Cibernética

Fonte: o autor, 2019.

Se alguma ação não se enquadra aí, não precisa fazer. Em azul, estão as quatro áreas temáticas: Estado e Sociedade; Efetividade; Colaboração; e Capacidades. A cibernética é transversal a tudo e na cibernética vale aquela explicação de que o oficial do QEMA (Quadro do Estado-Maior da Ativa) é capaz de resolver problemas do alfinete

ao foguete passando por pequenas cirurgias. Isso gera o quê? Uma multiplicidade de atores ou *stakehoders* e um número igual de linhas de comando e subordinação.

Conclusão número 1: é muito difícil estabelecer uma governança para isso. Você vai de setor em setor do governo, vai aos setores privados e vai se deparar que é difícil gerar legitimidade e autoridade para o estabelecimento de uma governança. Eu não posso dar uma ordem no Banco BRADESCO do tipo: Olha, utilize esse sistema ao invés desse, não faça isso, opera daquela maneira. Não posso fazer isso porque é privado. Por isto, as palavras mais lidas na literatura especializada em cibernética são: colaborativo, efetividade e capacidades.

Dentro de cada área temática, há alguns temas importantes. Outra palavra bastante empregada na cibernética é: resiliência. Por que resiliência? É impossível ou virtualmente impossível garantir 100% de eficácia nas ações de proteção cibernética. Isso quer dizer o quê? Se você for o alvo, você será atacado, lamento informar. Se o *hacker* quiser atacar aquele sistema ou aquela pessoa, ele saberá o que é necessário para controlar o seu celular. Basta saber o número do telefone. Diante dessa realidade, os americanos discutem muito se vale mais investir na proteção ou se vale mais investir na resiliência. A resiliência, por seu turno, possui dois vetores. O primeiro vetor é um sistema que precisa ser capaz de atuar e prestar o seu serviço, mesmo sendo degradado. O segundo vetor se traduz na necessidade de recuperação desse sistema o quanto antes.

Com relação à efetividade, preciso ter estruturas que me dêem esse resultado. Resultados que não servem para nada, não me interessam.

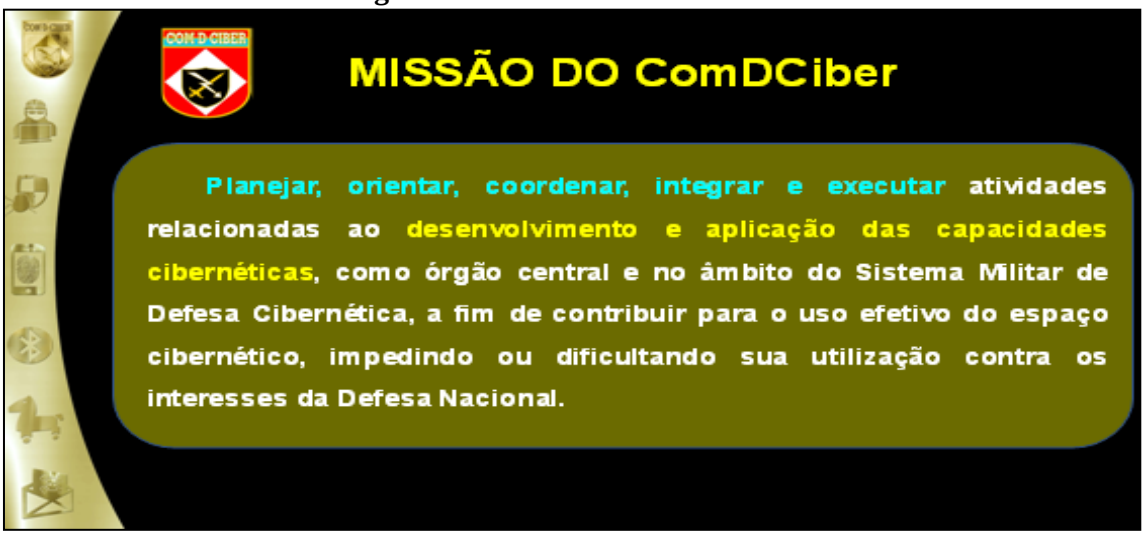
Em termos de capacidade, estão aqui os cinco pilares básicos da atividade cibernética: 1) inteligência; 2) ciência e tecnologia; 3) operações; 4) doutrina; e no centro, o grande paradoxo da cibernética 5) as pessoas. As pessoas são a maior vulnerabilidade, porque são elas que irão clicar num *link* malicioso, são elas que irão espetar um *pen drive* numa rede, naquela usina de *Natanz*, que sofreu um ataque pelo *Stuxnet.* Ao mesmo tempo, o ser humano é o maior recurso que nós temos para nos contrapor a essas ameaças.

O objetivo síntese do ComDCiber é ser um Comando Operacional Conjunto, permanentemente ativado, com capacidade operacional plena. Porém, esse objetivo ainda não foi alcançado, pois o ComDCiber ainda não tem estrutura física e pessoal para isso.

Já estamos operando 24/7, mas com uma estrutura que não é a nossa capacidade operacional plena. Além disso, há a necessidade do ComDCiber operar sob a forma de interagência, haja vista a necessidade de proteger as infraestruturas críticas.

Após a realização de todos esses estudos e análises, chega-se a seguinte missão do ComDCiber:

Figura 6 - Missão do ComDCiber



Fonte: o autor, 2019.

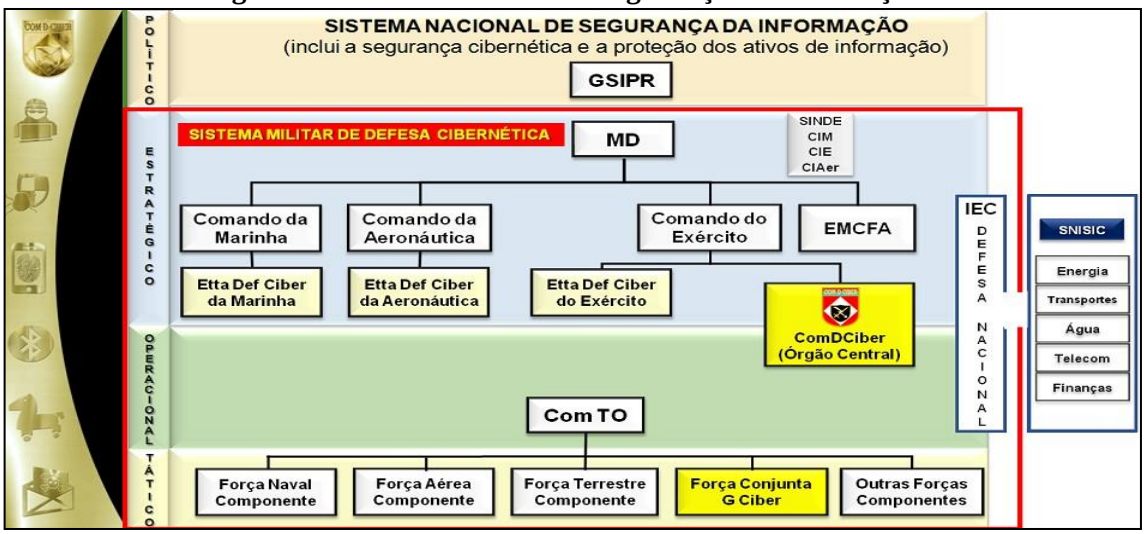
Diante do exposto, destaco um aspecto central no âmbito do sistema militar de defesa cibernética: o SISDABRA (Sistema de Defesa Aeroespacial Brasileiro), que por sua vez possui o COMDABRA (Comando de Defesa Aeroespacial Brasileiro). De maneira semelhante a essa estrutura, havia uma idéia inicial de tentar fazer um SISBRADECIBER (Sistema Brasileiro de Defesa Cibernética), tendo o ComDCiber como órgão central. Era a idéia inicial, mas a conclusão que chegamos é que seria difícil porque a defesa aeroespacial não é tão transversal a tudo.

E a quem interessa à defesa espacial brasileira? A todos nós cidadãos brasileiros é claro. Mas quem está envolvido nisso? Pouca gente na defesa aérea, na defesa antiaérea. Em suma, são sistemas muito específicos. Já na cibernética não, seria muito complicado assumirmos em âmbito nacional uma responsabilidade sobre os sistemas dos quais não temos controle. Ou seja, é uma situação bastante complicada e que requer muito estudo. Mas essa é a decisão. De alguma forma, nós podemos abrigar as estruturas críticas.

O ComDCiber tem a visão de futuro desenhada, que é basicamente atingir a capacidade operacional plena em termos de estrutura física, de procedimentos, de ferramentas e de pessoal. Hoje, o ComDCiber está com um efetivo bastante reduzido em relação ao previsto, mas não adianta receber todo mundo de uma vez, porque o ComDCiber não possui espaço físico para isso. Nós temos que acertar uma série de coisas e estamos implantando a capacidade aos poucos.

No que concerne ao sistema nacional de segurança da informação, o país está estruturado da seguinte maneira:

Figura 7 - Sistema Nacional de Segurança da Informação



Fonte: o autor, 2019.

No nível político, a principal ação é a proteção de infraestruturas críticas. Tendo a Secretaria de Assuntos Estratégicos (SAE) como o principal ator, o qual exerce um grande papel como elemento que insere esse assunto na agenda do governo, dando prioridade no orçamento. Passando para o sistema militar de defesa cibernética, verifica-se o ComDCiber como órgão central, que está subordinado ao Exército Brasileiro, haja vista que a Marinha do Brasil está responsável pelo setor nuclear e a Força Aérea Brasileira pelo setor espacial.

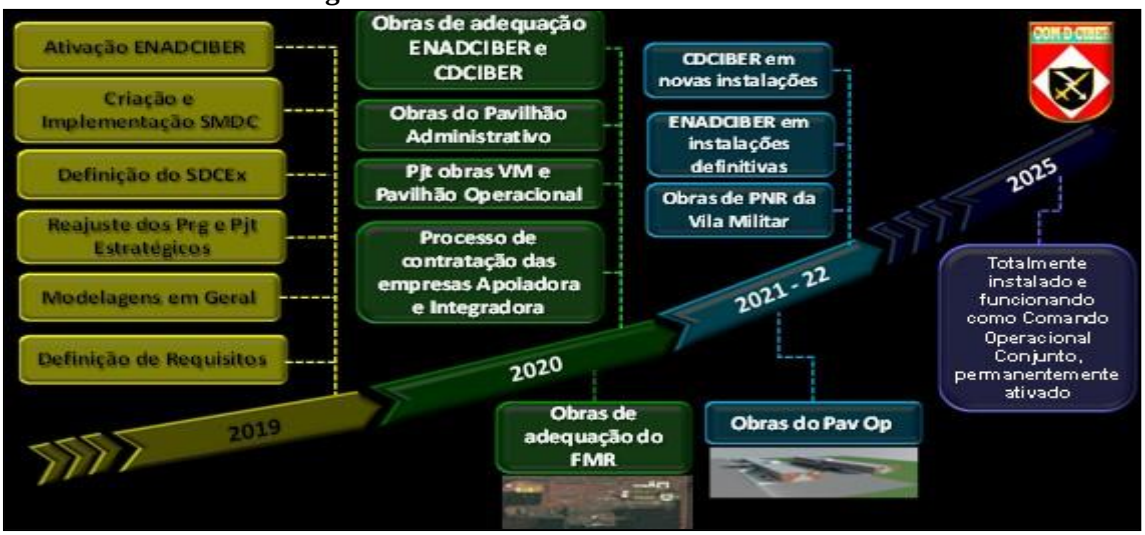
Observem o Estado-Maior Conjunto das Forças Armadas (EMCFA) e as estruturas singulares de cada força de defesa cibernética. Cada uma tem a sua. Há também o sistema de inteligência de defesa, que é um ator fundamental. A inteligência de fonte cibernética é muito importante, pois lida com a fonte humana, com a fonte de sinais, com a fonte de imagem e com a fonte cibernética. Dessa forma, é importante que esteja nesse sistema e na parte operacional. Na sequência, há o Comando do Teatro de Operações, com suas respectivas Forças Componentes, a Força Conjunta de Guerra Cibernética e outras Forças Componentes.

O Grupo de Segurança Institucional (GSI), por seu turno, é o grande responsável pela parte de legislação, que gera reflexos em todo o sistema de defesa nessa atividade. Por sua vez, o Estado Maior Conjunto das Forças Armadas é o principal ator no que tange as operações conjuntas e normativas no âmbito Defesa, ainda que a mesma tenha delegado ao Exército Brasileiro a condução disso. As estruturas singulares das três Forças Armadas (Centro de Inteligência da Marinha, Centro de Inteligência do Exército e Centro de Inteligência da Força Aérea) fornecem o apoio necessário para o desenvolvimento e para a aplicação das capacidades cibernéticas e da inteligência de fonte cibernética.

Estas são as palavras que marcam e emolduram a nossa colaboração com a proteção cibernética de estruturas críticas: cooperação e integração. Não somos responsáveis, mas cooperamos e integramos esforços nessa proteção. Em caso de ativação da estrutura militar de guerra, há uma minuta que foi praticada na Operação Amazônia este ano. O ComDCiber está sendo colocado nessa estrutura no mesmo nível que o Comando de Operações Aeroespaciais (COMAE), Comando do Teatro de Operações (COM TO) e o Comando da Zona de Defesa (COM ZD).

Dessa forma, o ComDCiber também possui um plano horizonte para os próximos anos, o qual é apresentado a seguir:

Figura 8 - Plano horizonte do ComDCiber



Fonte: o autor, 2019.

É claro que a nossa série histórica de orçamento é baixa. Não restam dúvidas de que o setor nuclear e o setor espacial são importantes, fundamentais e estratégicos. De um lado, o setor nuclear e o setor espacial possuem orçamentos anuais na ordem de 1,2 bilhões e 900 milhões respectivamente. E de outro lado, o setor cibernético conta com um orçamento infinatamente inferior, cerca de 7 milhões anuais. Tal fato se deve porque que a demanda do setor cibernético não estava estruturada. Se por um lado, ficamos preocupados em adquirir todas as capacidades necessárias, por outro lado não conseguimos estruturar ainda uma demanda que nos desce e nos possibilitasse chegar ao mesmo patamar de investimento praticado pelo país no setor nuclear e espacial.

De toda sorte, estimo que sejam necessários recursos na ordem de 150 milhões por ano, algo que é uma boa notícia. Ou seja, a cibernética é barata. É barata para quem ataca e barata para quem defende. Para isso, há dois programas estratégicos: um que nasceu em 2010 (Programa de Defesa Cibernética) e outro que nasceu em 2014 (Programa

da Defesa Cibernética na Defesa Nacional). Atualmente, o ComDCiber e o Estado Maior do Exército estão realizando estudos para fazer alguns reajustes.

Quer dizer que estávamos errados? Não. Simplesmente o quadro que nós temos hoje é formado por uma sucessão de escolhas e decisões que foram tomadas em momentos distintos, de acordo com a maturidade que havia em cada época em termos de cibernética, bem como a maturidade que havia em cada época na gestão dos projetos e dos programas estratégicos. Fato é que hoje o país tem outra maturidade em cibernética, outra maturidade na gestão dos programas estratégicos e a circunstância é outra também. Então é preciso ajustar. Eu tenho a mais clara certeza de que daqui a cinco anos, vai ter alguém falando de que o setor também está precisando de ajustes.

Vejam só a nossa ligação. Nós temos aqui ligações com o INMETRO, com o SENAC, com a ITAIPU, com pólos tecnológicos, com a Universidade Federal de Pernambuco, etc. Isso é resultado de um trabalho que foi feito junto a uma empresa, que faz uma consultoria para levantar a arquitetura de processos do ComDCiber.

Já temos um Fórum Ibero-Americano de Defesa Cibernética (o 3º fórum foi realizado esse ano no Brasil). Há uma reunião por ano e um exercício por ano. Conversei com o embaixador Candeias. Ele esteve no ComDCiber há pouco tempo e falou a respeito de pendurar esse Fórum dentro de uma iniciativa maior (ibero-americano), a nível governamental. É um fórum interessante de colaboração entre os dez países que participam.

Participamos de todas as operações conjuntas e combinadas. Países da OTAN podem se filiar ao Centro. Este ano a Coréia do Sul e o Japão estão com as presenças praticamente confirmadas. Da mesma forma, temos planejado para o ano que vem um trabalho grande de atividades. Todavia, as propostas precisam receber o apoio do MRE.

O ComDCiber participou esse ano de um exercício com uma equipe brasileira subordinada a uma equipe espanhola. No próximo ano, o ComDCiber participará sob a subordinação da equipe portuguesa. Já em 2021, a proposta é que seja uma equipe combinada composta pelos três países: Portugal, Espanha e Brasil. É muito importante, pois atualmente não há regimes internacionais que falem de cibernética, mesmo a ONU estudando muito esse assunto.

Figura 9 - Participação do Brasil em exercício Internacional

Fonte: o autor, 2019.

Esse ano vai ter de novo. Mas eu não tenho dúvida de que qualquer regime que aconteça, este Centro participará. Eu acho que isso é muito importante e não é muito custoso. E detalhe, o *staff* não é composto somente por militares. Pode ter acadêmicos, diplomatas, empresários, militares das Forças Armadas. Basta o Brasil pagar a quantia de 30 mil euros por ano para manter alguém nesse *staff*. É um passo importante para o Brasil se aliar a Estados importantes que tratam sobre esse assunto.

Esse exercício materializa a cooperação e integração na proteção de estruturas críticas. O exercício foi realizado entre os dias 2 e 4 de julho deste ano. Proteção cibernética dos setores elétrico, nuclear, financeiro, telecomunicações, defesa, águas e transportes.

Figura 10 - Exercício Guardião Cibernético 2.0

Fonte: o autor, 2019.

O Exercício Guardião Cibernético 2.0 foi um esforço do ComDCiber no sentido de incrementar a proteção do espaço cibernético brasileiro. O exercício contou com a

presença de mais de 200 participantes, oriundos de cerca de 40 instituições públicas e privadas, trabalhando juntos num evento cibernético. Nesta edição, o guardião cibernético contou com a participação de representantes dos seguintes setores: telecomunicações, elétrico, nuclear, financeiro e diversos órgãos parceiros de relevância para o cenário cibernético.

Durante esse período (2 a 4 de julho), os participantes atuaram de forma colaborativa e integrada, buscando prevenir e solucionar incidentes cibernéticos. Parlamentares e militares do Brasil e do exterior prestigiaram o evento. O objetivo central foi permitir uma interação do sistema militar de defesa cibernética com a proteção das infraestruturas estratégicas críticas do Brasil, através da criação de um cenário com problemas simulados de nível técnico e nível de gestão. Dois níveis de simulação foram trabalhados nesse exercício: 1) simulação técnica e construtiva; e 2) simulação virtual e construtiva. Havia desafios técnicos para todas as áreas. O gabinete de crise de cada empresa gestionava as questões inerentes aos ataques sofridos e as suas consequências, junto com os órgãos parceiros presentes no exercício.

Em síntese, a interação entre os participantes permitiu melhorar o nível de proteção cibernética dessas infraestruturas críticas. Para os participantes, o evento foi uma forma importante de compartilhar o conhecimento.

3. Conclusões

Em ultima análise, a ameaça cibernética é muito capaz, presente e atual. Aumentar essa resiliência na sociedade é importante para que possamos nos conduzir de maneira mais segura nesse ambiente altamente tecnológico de hoje em dia.

Nenhuma corrente é mais forte que o seu elo mais fraco. A nossa proteção é semelhante a isso. Ela começa na escola fundamental ensinando as crianças o que é a *internet*, como elas devem fazer uma senha, que as pessoas não são boas como o pai e como a mãe, etc. Coisas erradas passam pela rede *wi-fi* da casa de cada um de nós. É muito simples a programação da rede *wi-fi* da sua casa aumentar absurdamente o nível de segurança. Sempre que alguém quiser, vai entrar na sua rede. Mas se você for colocando camadas de proteção, vai oferecer resistências diferentes em cada camada, pelo que vai dificultar e aumentar o custo para que alguém consiga entrar na rede.

E no âmbito nacional, a proteção da nossa sociedade passa pela preocupação de cada um de nós em colocar as camadas de segurança e de proteção necessárias para que

as mesmas possam fazer frente aos ataques cibernéticos. Feito isso, vocês vão contribuir enormemente para o meu sono tranquilo.

Muito obrigado!

CIBERESPAÇO NO CONTEXTO DA GUERRA DO FUTURO: UMA VISÃO DA ACADEMIA

Avelino Francisco Zorzo*

1. Introdução

Bom dia a todos.

Antes de começar a minha palestra eu só gostaria de fazer uma pergunta aqui na platéia: Todos vocês tem um computador? Todos. Todos vocês tem um celular? Todos têm um celular e um computador. Quem tem um cartão de crédito? Todos têm um computador, um celular e um cartão de crédito hoje em dia. Um aparelho celular nos dias atuais não é apenas um mero telefone. Como ele pode ter de dois a três processadores internos, memória volátil, memória não volátil, ele se consiste um computador.

Hoje em dia há computadores espalhados em todas as áreas do conhecimento. Independente da forma como a computação é tratada, o aspecto da segurança precisa ser levado em consideração, senão o país pode ser parado.

O mundo muda muito, ele está sempre mudando. Desde os primórdios da humanidade, o mundo vem mudando e as tecnologias seguem a mesma tendência. A grande diferença nos dias atuais é que essas mudanças são muito rápidas. Se voltarmos 20, 30 anos atrás e pensarmos como era a sociedade nesse período, chegaremos à conclusão de que ela era completamente diferente da sociedade dos dias atuais. Então, devemos estar sempre preparado com as mudanças que estão acontecendo. Mas, como fazemos num mundo que está em constante transformação?

A minha apresentação é voltada para a preparação da academia para enfrentar as mudanças mundiais e como nós deveríamos estar olhando para a academia. A sociedade está preparada para esse mundo ali na frente, mas poderia dizer até o mundo de hoje.

2. Desenvolvimento

A figura a seguir é instigativa na medida em que proporciona uma comparação interessante. Ou seja, ao se comparar o mundo real atual com o mundo real de algumas centenas de anos atrás, será verificado que as pessoas daquela época não conheciam o mundo real atual, que as pessoas não conheciam todas as leis da física, que as pessoas

* Doutor em Ciência da Computação, Coordenador de Programas Profissionais na CAPES e Professor Titular da Pontifícia Universidade Católica do Rio Grande do Sul.

não conheciam as propriedades da química, que as pessoas não conheciam biologia, enfim, que as pessoas não conheciam diversos aspectos que trouxeram significativos avanços para a sociedade e que hoje estamos habituados com essas contribuições. E com o passar do tempo, as pessoas estudaram esse mundo real e começaram a entender um pouco o que é o mundo nos dias atuais. Então, hoje a sociedade sabe como o fogo se forma, como se comporta o corpo humano, o porquê do avião se levantar, etc.

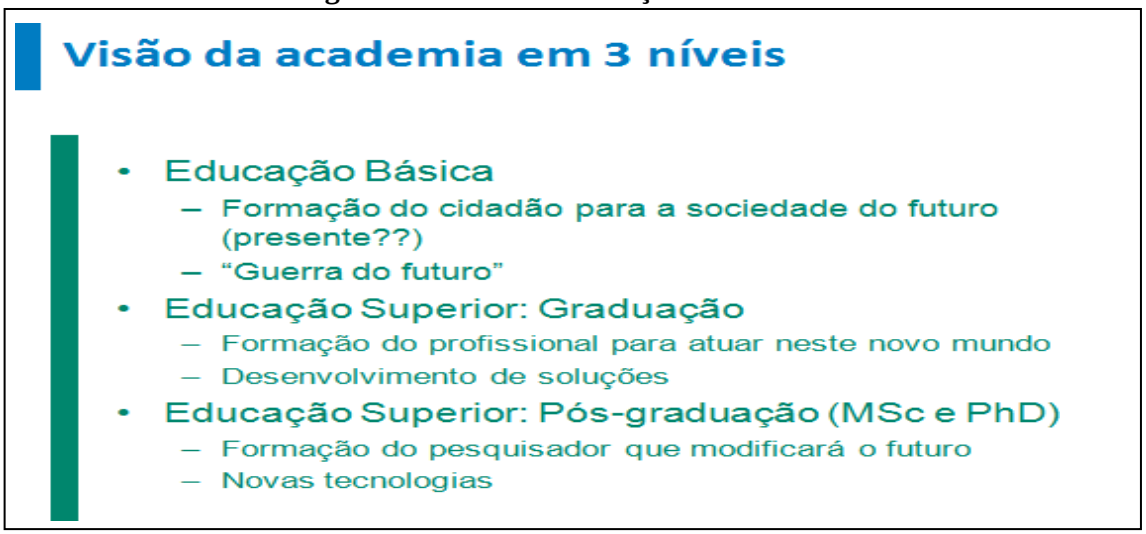
Figura 1 - Mundo em mudanças

Fonte: o autor, 2019.

Entretanto, ao se analisar o mundo virtual, iremos nos perguntar sobre quantas pessoas, efetivamente, conhecem esse mundo virtual. O mundo virtual é completamente diferente de tudo que já aconteceu. Se voltarmos algumas centenas de anos, iremos constatar que as pessoas daquela época achavam que o fogo era mágico e se teletransportarmos as mesmas pessoas dessa época para os dias atuais, elas também acharão que o envio de mensagens para qualquer pessoa do mundo é uma mágica também. O mundo virtual tem diferentes aspectos que as pessoas não entendem. O *ciberespaço* é o principal palco da guerra do futuro. E nesse aspecto, as pessoas não estão preparadas para enfrentar esse mundo. Todavia, elas estão muito mais suscetíveis aos ataques se resolverem fazer soluções imcompatíveis com esse mundo.

Se voltarmos para o mundo real, quantas pessoas trabalham, vivem nesse mundo e não sabem o que está acontecendo e nem tampouco conhecem o mundo virtual? Esse é um trabalho que vem sendo realizado há alguns anos na Diretoria de Educação da Sociedade Brasileira de Computação (SBC). Até 2015, atuei como Diretor de Educação da SBC, quando começamos a discutir com o Ministério da Educação essas questões. Afinal, se o país não preparar o jovem para atuar nesse mundo, imagina como será a sociedade daqui a alguns anos:

Figura 2 - Níveis de educação cibernética



Fonte: o autor, 2019.

Se olharmos para outros países, poderemos ver que diversos países já possuem este tipo de ensino, que abarca desde a educação básica até a pós-graduação. Anos atrás, o próprio *Barack Obama* foi à televisão e solicitou a população norte-americana ajudar na construção desse tipo de educação, porque esse é o futuro. Todavia, as pessoas não têm a noção de que tipo de profissional, a sociedade precisa formar para atuar nesse mercado.

Diante dessa realidade, destaco que vou falar também sobre um possível currículo para a formação de profissionais que atuam nesse segmento de mercado. Que disciplinas e conhecimentos interdisciplinares são necessários. E por último, vou falar um pouquinho sobre as pesquisas e mostrar como as universidades estão trabalhando em pesquisas na área de segurança. Será apenas uma amostra pequena, uma vez que no Brasil há mais de seis mil projetos de pesquisa em curso na área de computação.

Em relação à educação básica, verifica-se que há três aspectos da computação, os quais buscam compreender como a computação pode ajudar e como as crianças têm que aprender isso desde o ensino fundamental. Esse é um trabalho que a sociedade brasileira de computação faz junto ao Ministério da Educação desde 2015. Trata-se de uma proposta que busca inserir essa matéria no currículo da educação básica. As crianças precisam estar preparadas para esse mundo e se procurar na base nacional comum curricular, vai poder encontrar esse material. Ele deve ser tratado em todas as escolas do Brasil. As pessoas que trabalham com isso sabem que a computação não é uma abstração.

Outro aspecto importante, notadamente no setor de segurança cibernética, é a compreensão adequada da formação do mundo digital. Quais artefatos são produzidos por essa revolução digital? O que tem acontecido nesse mundo digital e o que é esse mundo

digital? O que é a internet? Como ela funciona? Como é que a gente faz com os protocolos de segurança? Por que alguém consegue burlar aqueles protocolos de segurança? E quais os requisitos que a gente precisa ter nos equipamentos para que ele não sofra uma pane?

Com base nessa realidade, chegou-se nesses três eixos da computação e como cada um trabalha nesses aspectos: pensamento computacional, mundo digital e cultura digital.

Figura 3 - Eixos da computação na educação básica

Fonte: o autor, 2019.

O pensamento computacional está voltado para a resolução de problemas e suas principais características são a abstração, a automação e a análise.

Já o mundo digital, nota-se que o mesmo é caracterizado pela codificação, processamento e distribuição. Como isso é processado? Quais problemas podem ser resolvidos pelo computador? Quais problemas não podem ser resolvidos dentro de uma máquina? Porque quebrar a criptografia assimétrica? Se ela for bem feita, eu posso levar algumas centenas de milhares de anos para tentar resolver essa questão.

A cultura digital é algo que precisa ser desenvolvido pela população em geral e se pauta por três aspectos, a saber: computação e sociedade, fluência tecnológica e ética digital. Quando as pessoas recebem uma mensagem pelo *whatsapp*, primeiramente precisam verificar se a mensagem é verdadeira ou se falsa. Como é que elas fazem para se blindar daquele tipo de situação?

No início, constatei que 90% a 100% das pessoas presentes neste auditório possuem um celular. Isso quer dizer que 90% e 100% das pessoas presentes aqui estão conectadas neste momento e cada uma é um potencial ponto de ataque. Quantos de vocês efetivamente lêem os termos de aceite de um aplicativo quando baixam os mesmos em seu celular? Se vocês não lerem aquele aplicativo, suas vozes podem estar sendo

coletadas. O aplicativo pode estar instalando coisas que você não sabe. Ele pode está coletando imagens sem você saber. Ou seja, tudo isso que a gente está falando aqui pode estar sendo executado em algum desses celulares aí sem a gente saber. Além disso, o aplicativo pode estar enviando essas informações para algum lugar que a gente não sabe. Mais de 90% da população brasileira não entende isso. E os 10% que entendem, tomam essa atitude mesmo assim. Em suma, acredito que a grande maioria de vocês entende os riscos que estão correndo, mas fazem mesmo assim.

Precisamos desenvolver a questão da cultura digital na sociedade. Se olharmos para a sociedade, verificaremos que ela está completamente mudada. Hoje, o mundo está diferente do que há vinte anos atrás. As redes sociais mudaram o comportamento das pessoas. Nos dias atuais, consegue-se atacar uma sociedade de uma maneira muito mais fácil. Não é mais necessário a realização de um ataque com uma bomba, basta manipular a população. É possível alterar o comportamento de um país inteiro através de mensagens. O ataque não precisa estar voltado para uma infraestrutura, ele pode ser direcionado à população por meio de mensagens.

A gente tem que estar preparado para entender isso. Dessa forma, entendo que as pessoas irão entender essa realidade somente se receberem educação adequada desde o nível básico. Se as pessoas não entenderem isso, elas serão manipuladas de uma maneira muito mais efetiva.

Quem já ouviu falar em robôs? Os robôs que estão na *internet*. Quem já acessou o *site* de compras, onde o mesmo apresenta um valor de um determinado produto e daqui a cinco minutos, o mesmo produto sobe de preço? Isso ocorre para que as pessoas comprem. Os robôs ficam manipulando os valores para fazer com que as pessoas comprem o produto. Imaginem os algoritmos que controlam uma rede social? Eu posso ter um algoritmo que manipula determinada informação para um conjunto de pessoas que eu quero disponibilizar.

Isso tudo que eu falo para vocês é algo que a gente deveria ver desde a educação básica. Atualmente, as crianças já usam a tecnologia, elas são fluentes digitais, mas muitas vezes não entendem tudo que está por trás. Sob o ponto de vista da academia, se a sociedade quer chegar nesse mundo, é necessário prepará-la para isso, porque de nada adianta adotar uma postura defensiva.

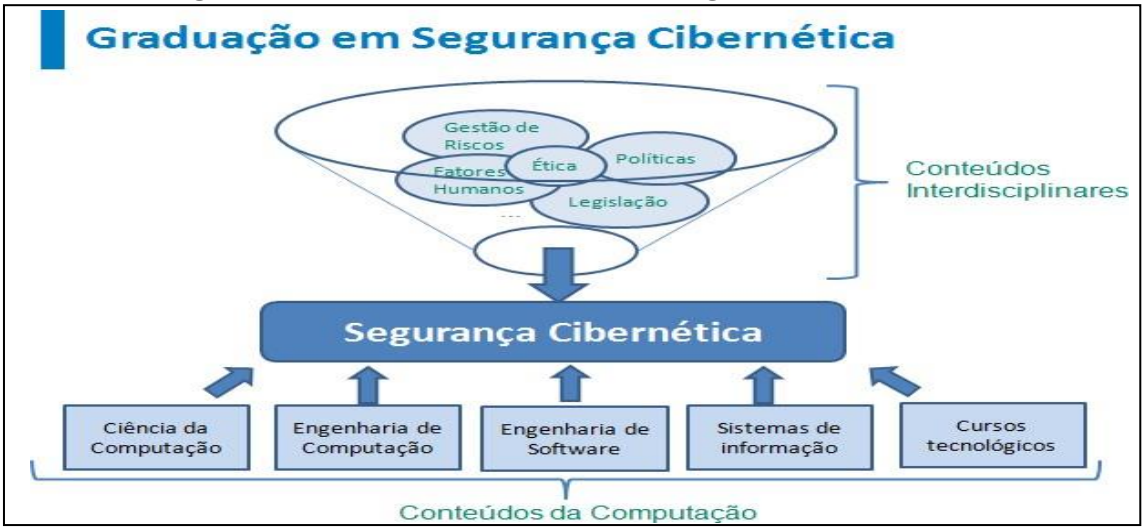
No tocante ao ensino superior, verifica-se que a população precisa ser preparada desde os níveis mais básicos, inserindo conceitos importantes ao longo dos anos de tal forma que cheguem nas universidades preparadas para o campo profissional. Existe um

trabalho que é feito na comissão especial na área de segurança da informação da SBC. Trata-se de um simpósio brasileiro na área de segurança da informação e segurança computacional que ocorre anualmente há mais de 10 anos. Nele, os pesquisadores brasileiros discutem o que está sendo feito de pesquisa na academia.

No Brasil há 56 cursos de graduação. No exterior, há também diversos cursos que a gente chama de tecnológico, duram em média de quatro a cinco anos. A comunidade acadêmica internacional e a indústria têm discutido sobre o tema em pauta e verificaram que a sociedade precisa de 22 tipos de profissionais novos.

Por exemplo, hoje estamos gerando dados nessa sala mesmo, alguns *megabytes* ou *gigabytes* de informação estão sendo transmitidos sem a gente saber, a não ser que os celulares estejam desligados. Mas, mesmo assim ele fica coletando e depois manda essas informações. Nesse sentido, há o profissional conhecido como *cibersecurity*. Os conhecimentos necessários para alguém atuar nessa parte de *cibersecurity* estão divididos em duas partes: 1) conhecimentos disciplinares (área de computação); e 2) os conhecimentos interdisciplinares (os conteúdos que são interdisciplinares):

Figura 4 - Conteúdos desenvolvidos na segurança cibernética



Fonte: o autor, 2019.

A figura anterior nos mostra que os conteúdos interdisciplinares envolvem aspectos sociais, legislação, ética e diversos assuntos diferentes da área de computação.

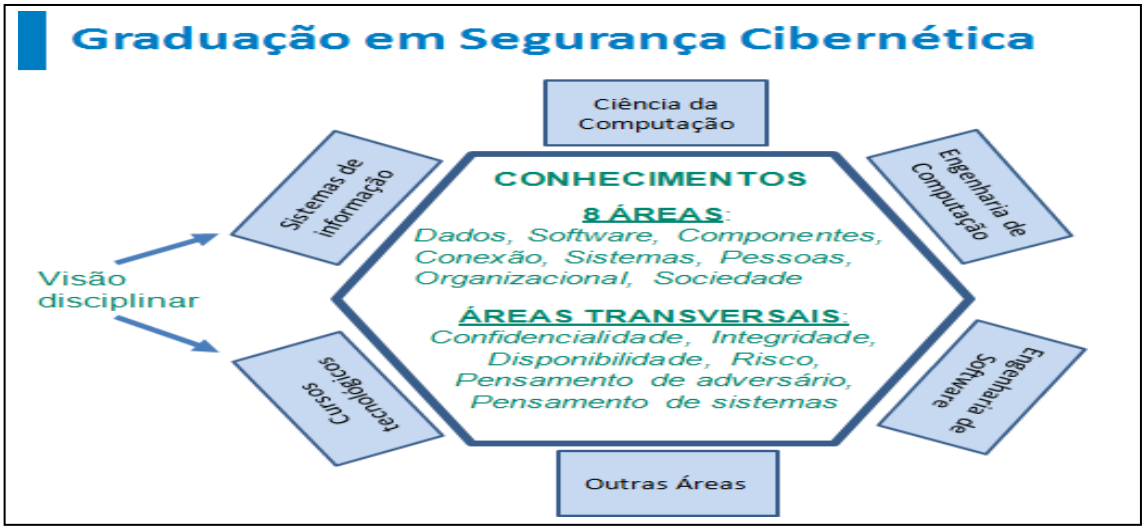
Agora, imaginem se a gente tiver um conjunto de egressos do ensino médio e do ensino básico que já venham com parte desse conhecimento? Quando eles atuarem nesse ambiente, estarão muito mais preparados para entender todos os fatores que foram citados.

Mas em geral, os ataques ocorrem no elo mais fraco da corrente, que são os 90% da população que eu falei anteriormente. Quando baixamos os aplicativos sem lerem os termos, estamos suscetíveis a ataques. Quando recebemos *emails* desconhecidos, estamos suscetíveis a ataques, basta clicar no item solicitado, que o usuário irá instalar um aplicativo que coletará suas informações pessoais. Ou seja, os fatores humanos são fundamentais.

Se vocês ouviram falar de enigma, poderão constatar que se tratava de uma máquina de criptografia utilizada pelos alemães na 2ª GM. Se vocês leram um pouco sobre ela, vocês verão que um dos motivos que o pessoal em *Bletchley Park* tentava decifrar as mensagens, era porque os operadores do enigma eram preguiçosos. Eles repetiam a mensagem do dia diversas vezes e às vezes utilizavam as iniciais da namorada, do pai ou da mãe.

Não há tantos cursos no Brasil, como nos EUA e na Europa. Em geral, o Brasil possui esses cursos na área de computação:

Figura 5 - Graduação em Segurança Cibernética no Brasil



Fonte: o autor, 2019.

O primeiro curso é a ciência da computação, que tem enfoque voltado para a resolução de problemas em geral (computação gráfica, teoria da computação, engenharia de *software*, redes de computadores, segurança, criptografia). O segundo curso é a engenharia de computação, que é uma mistura da engenharia elétrica, da engenharia eletrônica, da computação e parte do desenvolvimento de *hardware.* O terceiro curso é a engenharia de *software*, que é o desenvolvimento de *software* como produto. O quarto curso são os sistemas de informação, que nada mais é do que o caminho necessário para levar a infraestrutura de *hardware* e *software* para dentro das organizações. Há também os cursos tecnológicos e as outras áreas que tangenciam a área cibernética. Ou seja, no

Brasil há uma dezena de cursos (desde a segurança cibernética até o desenvolvimento da *web*, desenvolvimento da internet, rede de computadores, banco de dados e assim por diante).

Para a confecção do currículo na área de segurança cibernética, torna-se necessário apoiar-se nos currículos dos diversos cursos da área de computação existentes. Basicamente são oito áreas de conhecimento. Há os conceitos transversais: confidencialidade, integridade, disponibilidade, risco, pensamento de adversário e pensamento de sistema. Feito isto, teremos uma visão interdisciplinar de cada uma das disciplinas das oito áreas de conhecimento.

Há diversas formas para cada uma das áreas do conhecimento. Para cada uma delas, há um conjunto de conhecimentos que são necessários tanto para a segurança de *software*, como para a segurança de componentes, como para a segurança de conexão, como para a segurança de sistemas, como para a segurança de pessoas, como para a segurança organizacional e como para a segurança da sociedade. Cada um desses aspectos é fundamental para que eu possa ter um profissional que realmente entenda o que estará fazendo nessa área de *cibersecurity*.

A partir de agora, vou discorrer sobre a educação superior no Brasil na área de computação:

Figura 6 - Distribuição regional de cursos

Fonte: o autor, 2019.

Temos um conjunto de cursos espalhados pelo Brasil, concentrados fortemente no litoral. Em Pernambuco, por exemplo, há os cursos de Mestrado, Mestrado profissional e de Doutorado em *cibersecurity*, seja em nível de rede, seja em nível dos sistemas operacionais, seja na parte de segurança de dados, segurança da informação e assim por

diante. Além disso, atualmente existem 123 cursos de pós-graduação (Mestrado e Doutorado) em funcionamento no país, pelo que já resultou na formação de 272 Doutores e 1.255 Mestres em cibernética no país. Esses resultados foram obtidos no relatório da avaliação quadrienal de 2017.

Existem algumas universidades que seguem a tendência mundial, principalmente as mais antigas, e estão formando mais Doutores do que Mestres. Em geral, no mundo praticamente não há cursos de Mestrado, o foco se baseia em ofertas para cursos de Doutorado. Estamos no momento de realizar uma avaliação intermediária dos programas de pós-graduação no Brasil, pelo que analisei os dados coletados referentes aos anos de 2017 - 2018 e procurei as linhas de pesquisas que têm relação com o tema:

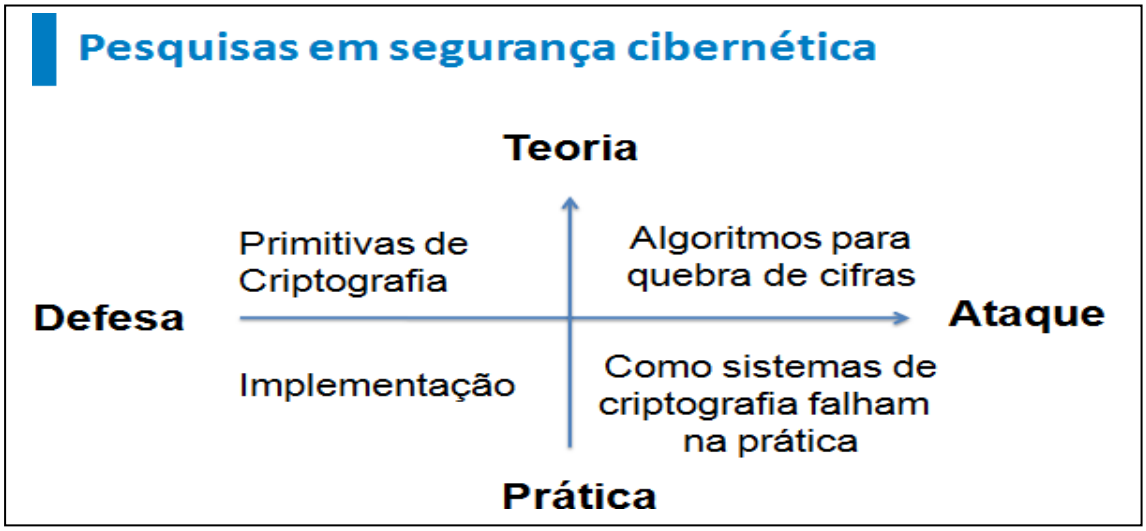
Figura 7 - Pesquisas nos Programas

Fonte: o autor, 2019.

O tamanho das letras representa o número de projetos que as universidades possuem dentro das linhas de pesquisa. Não necessariamente significa que todos os projetos são exatamente na área de segurança. Pode ser notado que existe um conjunto bem grande de universidades atuando em pesquisa na área de segurança da informação no país. Isso é só um pequeno exemplo, há muito mais do que isso.

O gráfico a seguir representa as ações que podem ser feitas numa pesquisa. Podemos atuar desde a defesa ao ataque, ou seja, na defesa como é que eu me protejo para não ser atacado e no ataque é o que eu vou fazer para atacar alguém, para destruir a infraestrutura e para capturar alguma informação do outro lado:

Figura 8 - Gráfico conceitual das pesquisas



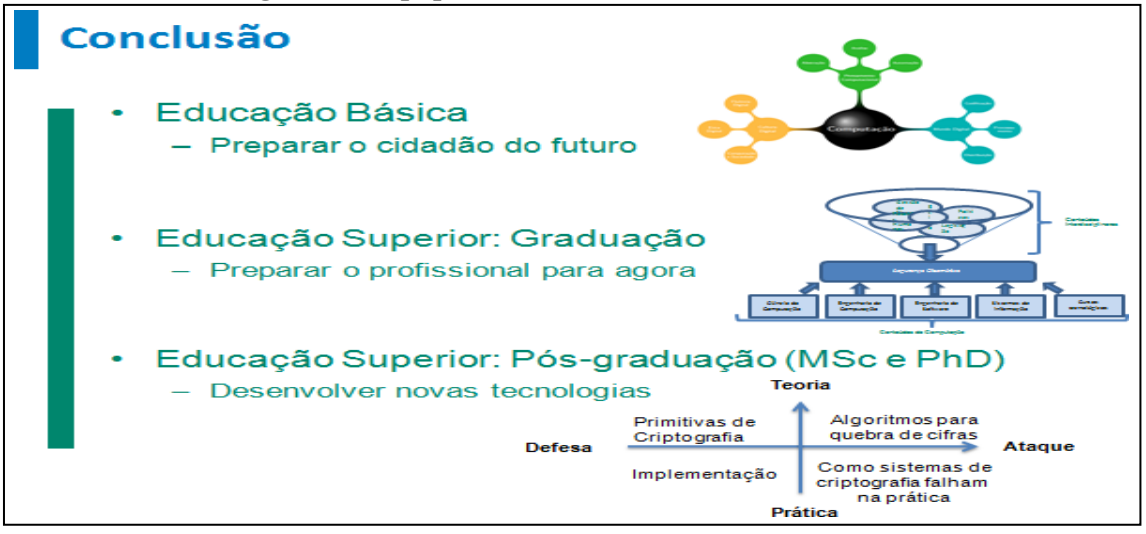
Fonte: o autor, 2019.

Assim, cumpre destacar que não há nenhum algoritmo que teoricamente seja seguro. Todos, teoricamente, são possíveis de quebrar. A questão é que essa ação pode levar algumas centenas de anos ou alguns milhares de anos para ser concretizada. Na teoria o algoritmo é suscetível a ataques, mas na prática não é.

3. Conclusões

Para concluir, procurei mostrar uma visão do que está acontecendo na academia e como é que a gente tem que preparar as pessoas para um cenário futuro, que eu tentei mostrar para vocês. Em síntese, a solução para esse desafio é a preparação do nosso aluno desde a educação básica, para que ao longo dos anos ele adquira e amadureça os conhecimentos necessários sobre o ambiente cibernético, coforme a figura a seguir:

Figura 9 - O papel da educação na área cibernética



Fonte: o autor, 2019.

Não tem como, iremos sofrer ataques cibernéticos a todo instante, sem percebermos. Às vezes, precisamos refletir de como iremos preparar esses profissionais.

Que tipo de curso de graduação será necessário para que os profissionais possam atuar nesse ambiente? Quais são as pesquisas necessárias para obtenção de novas tecnologias e que nos posicionem a frente?

Muito Obrigado pela atenção!

A CIBERNÉTICA SOB A PERSPECTIVA OPERACIONAL E EMPRESARIAL

Roberto Alves Gallo Filho*

1. Introdução

Senhoras e senhores, boa tarde.

Eu tenho múltiplos chapéus. O que vou expor não é necessariamente a visão de nenhum deles, mas é a minha visão. O primeiro chapéu se refere à parte profissional. Atualmente, sou o presidente da Associação Brasileira das Indústrias de Materiais de Defesa e Segurança (ABIMDE), órgão que congrega mais ou menos 200 empresas do setor de Defesa brasileiro. Temos a EMBRAER, AVIBRÁS, todo o tipo de empresas. A ABIMDE é muito representativa. Nesse *holding*, existem cerca de trinta empresas que possuem ofertas no setor de cibernética e guerra eletrônica ou na mescla de *cibereletrônica*. Outro aspecto importante é que não há somente empresas de capital de controle nacional atuando neste setor no Brasil. Há grandes empresas internacionais trabalhando em solo brasileiro, tais como a *Abbi System*.

O segundo chapéu se refere à área acadêmica. Da minha graduação ao pós-doutorado, fiz pesquisas voltadas ao tema de segurança cibernética. O meu último pós-doutorado foi na área de ensino de cibernética. O último chapéu se refere à parte empresarial. Sou fundador e sócio dessa empresa: *Kryptus shaping trusted bonds.*

Figura 1 - Kryptus shaping trusted bonds

Fonte: o autor, 2019.

* Doutor em Ciência da Computação e Presidente da Associação Brasileira das Indústrias de Materiais de Defesa e Segurança.

Trata-se de uma empresa especializada em segurança cibernética e criptografia. A *Kryptus* está presente em praticamente todos os projetos que envolvem Defesa no Brasil. Trabalho há quase 20 anos nesse setor. Dessa forma, o que eu vou falar não é necessariamente a opinião da academia ou da ABIMDE, mas provavelmente da *Kryptus,* porque sou o sócio fundador.

2. Desenvolvimento

O que é a guerra cibernética? Basicamente a guerra cibernética possui várias definições: ONU, OTAN, etc. A minha definição de guerra cibernética é mais simples, consiste basicamente em explorar a vulnerabilidade dos sistemas com o intuito de causar a interrupção ou negar o espaço cibernético. Em outras palavras, o objetivo da guerra cibernética é usar sistemas de informação para causar interrupção do próprio espaço cibernético ou influir no espaço cinético controlado pelo cibernético.

Há também outro conceito de guerra cibernética, que nada mais é do que o emprego da guerra eletrônica no expectro eletromagnético com o intuito de fazer algo interessante, como o bloqueio de uma comunicação de um alvo através do sinal daquele mesmo alvo. Por exemplo, tenho duas plataformas aéreas que estão se comunicando e ela tem um *datalink* comunicante com duas plataformas. Quero que o meu adversário não tenha capacidade de coordenação. Então, eu vou lá e por meio de ações, atrapalho isso. A guerra cibernética também pode ser empregada para causar interrupção no campo de batalha por meio de várias ações.

Um caso interessante foi a operação combinada realizada entre a Marinha do Brasil e a Marinha da Inglaterra. Num certo momento, a emissão eletromagnética do porta-aviões inglês foi tão potente que queimou os sistemas computacionais da classe Tamandaré brasileira. Imaginem numa hipótese de ataque eletrônico? Ou seja, a guerra eletrônica tem um poder muito grande.

É impossível falar de guerra cibernética sem falar de guerra eletrônica. Tanto é que hoje o número de sistemas autônomos que envolvem os sistemas *ciberfísicos* é grandioso. No tocante ao sensoriamento, nota-se que os mesmos são, por essência, sistemas eletrônicos. Houve alguns casos envolvendo ataques cibernéticos e eletrônicos recentemente.

O primeiro caso diz respeito a atuação das forças militares norte-americanas no conflito da Síria. Trata-se de uma frota de 13 veículos aéreos não tripulados (VANTs) norte-americanos que foi utilizada para buscar e bombardear uma posição militar russa

na Síria. O discurso estadunidense é que eles não atuaram na operação. Fato é que metade desses drones foi abatida com baterias antimíssil e a outra metade saiu ilesa. Um ataque cibernético clássico, por assim dizer.

Não sei se vocês recentemente viram um *Global Hawk* que foi roubado pelos iranianos. Tal VANT custa algo em torno de 100 milhões de dólares. Um sistema de armas como esse utiliza uma frota composta de 13 VANTs, pelo que perfaz um total de 1,3 bilhões de dólares. Esse monatnte equivale basicamente ao programa da Força Aérea Brasileira do *Gripen*. Ou seja, os Estados Unidos da América (EUA) utilizaram esse montante para atacar a posição russa no conflito da Síria.

Eu tenho pesquisado e verifiquei a evolução desse assunto na doutrina norte-americana. Em meados de 2009, os EUA decidiram que cada Brigada da Força Aérea Americana deveria contar com um Destacamento de Guerra Eletrônica. Ou seja, cada Brigada da Força Aérea Americana deveria contar com homens que atuassem no campo cibernético. Se por um lado, verifiquei o emprego de profissionais especializados em cibernética nas forças militares norte-americanas, por outro lado, constatei que o Brasil está atrasado demais.

Há também a Austrália, que conta com um centro de pesquisa atuando em prol do goveno australiano. Todavia, o que é mais interessante dessa estrutura é a sua organização. Tem áreas de ação e o funcionamento entre elas é um *continuum*. Tem uma separação também. É o que a gente observa no ambiente puramente cibernético. Tem as operações clássicas, que variam desde a criptografia matemática, que é a área mais pura, até o outro extremo: as operações, que são o escopo do ambiente eletromagnético. Nesse caso, você fala até de ataques. Trabalha-se com várias hipóteses de emprego, etc.

Quando trazemos essa estrutura em prol das operações, precisamos enquadrá-la sob uma doutrina. Se por um lado, o militar precisa ser ousado no emprego da força, por outro lado precisa ser conservador no emprego de meios. Existem os teatros de operação (TO) clássicos: marítimo, espacial, aéreo e terrestre. Mas nos dias atuais, existem outros TO, tais como o cibernético. No ambiente cibernético, é importante que o General seja oriundo da arma de comunicações, porque a comunicação é por essência cibernética.

O meio cibernético e a guerra eletrônica expande cada vez mais a área de interesse no contexto das operações. O projeto COBRA, por exemplo, é um projeto que leva o meio *cibereletrônico* até a ponta da linha no campo de batalha. Nos dias atuais, todos os combatentes estão com uma câmera em seus capacetes. Tal medida foi tomada para que o soldado dê, em tempo real, a consciência situacional mais atualizada ao escalão

superior. Esse tipo de tipo de situação só tem aumentado e é fundamental que essas operações sejam entendidas como um exemplo a ser seguido.

Um aspecto importante a ser ressaltado é que não há coordenação entre as Forças Armadas Brasileiras. Enquanto uma determinada Força Armada opera com aparelhos MOTOROLA, outras operam com aparelhos HERTZ. Ou seja, falta muito para que o Brasil possa evoluir para um Teatro de Operações, onde as três Forças Armadas possam falar entre si.

O campo *cibereletromagnético* é uma integração interessante. Ele consegue observar todos os integrantes entrelaçados. O espaço eletromagnético está um pouco mais para o mundo físico e informacional. Já o *ciberespaço* está mais para o informacional e cognitivo. Essas dimensões estão presentes em cada um dos teatros de operações.

Outra forma de pensar é a reflexão de como eu monto operações. Não é que eu posso ter operações puras no *ciberespaço*, que são as operações mais difundidas na mídia. Eu posso ter operações que são exclusivamente eletromagnéticas: inteligência de sinais. Um exemplo clássico e que tem sido operado com sucesso é o emprego de um ataque cibernético precedendo um ataque cinético. Inicialmente, ocorre o ataque cibernético desabilitando toda a infraestrutura de defesa, até as telecomunicações do território inimigo e depois, ocorre o ataque cinético propriamente dito.

Um assunto importantíssimo são as armas letais e as armas letais autônomas. Há uma discussão muito grande sobre o que realmente seria isso. Alguém tem idéia de quando começou? Alguém tem idéia do por que do primeiro sistema autônomo letal? Alguém quer chutar livremente de como os torpedos da marinha de guerra alemã foram disparados na 2ª Guerra Mundial? Será que eles tinham um sonar e eles identificavam através do sonar ou será que os torpedos eram automaticamente enviados? Fato é que os sistemas autônomos vêm evoluindo desde meados do século XX e nas décadas de 1970, de 1980 e de 1990, ocorreu o grande salto.

Então o que diferencia o robô de um humano num campo de batalha? Na prática nada, porque ter um formato humanóide não torna o sistema letal autônomo menos letal ou menos autônomo. Talvez seja um pouco mais chocante para o pessoal saber a posição que tem sido tomada pela maior parte dos países em assuntos dessa natureza: a quase totalidade dos Estados é contra um tratado internacional que limite o uso de sistemas letais autônomos porque tem uma série de questões éticas ligadas. A posição brasileira é a de que se busque um tratado internacional que regulamente isso, segundo o exemplo da convenção de genebra e do Tratado de Não Proliferação de Armas Nucleares.

Mas, no sentido de sistemas autónomos, independente de ter um sistema que não precise de permissão, ainda assim precisa da intervenção humana. Ou seja, ele ainda depende do *input* humano. Basicamente, um sistema autônomo pode designar o alvo, informar que está pronto para o emprego de força e relatar que está em condições do operador humano. Esse tipo de assunto causa furor, pois já existem torpedos autônomos há muito tempo. Todos, porém, estão chegando e atacando cada vez mais. É a percepção pública.

Tem várias perguntas éticas que precisam ser enunciadas. Por exemplo, no caso de imputar responsabilidades, quem é o responsável pelo emprego inadequado de uma arma: o fabricante ou o comandante? Essas questões são muito difíceis de serem respondidas. Quando um combatente vai lá, aperta o gatilho e mata alguém, claramente o combatente tem um papel nessa história, ele pode ser culpado ou não, mas obviamente ele causou aquela morte. Agora, num sistema autônomo, esse tipo de pergunta fica bastante difuso. E a responsabilidade é uma das coisas fundamentais para a punição. É fundamental para o ser humano se comportar. Ou seja, é importante a pessoa saber que se fizer algo errado, pode levar uma pancada de volta. Isso é fundamental, porque senão isso acaba virando um video game.

Existe um projeto norte-americano bastante interessante. A ideia central desse projeto é que os EUA estão fazendo esquadrões híbridos, com o comandante sendo um ser humano. O projeto possui artefatos, robôs, drones, etc. Os drones atuam junto com a tropa para aumentar a consciência situacional da mesma, permitindo-a maior efetividade no emprego da força. Esses atores estão conectados com um *datalink* local. A inteligência artificial que auxilia isso é um exemplo de que não é com um desses robôs que se consegue fazer o reduto do ambiente. O PC do Comandante é o local onde o mesmo consegue observar a movimentação da tropa inimiga, da mesma forma que possui uma capacidade expandida de comunicação. O que se espera dentro desse projeto é que esses robôs engajem também contra o inimigo.

Outra coisa interessante é o vôo de treinamento. Como vou treinar pilotos e aeronaves se eu somente tenho uma aeronave para fazer o jogo de perseguição? Em vez de colocar outra aeronave e pilotos humanos para atuarem como inimigo, eu posso empregar sistemas autônomos para fazer o papel de aeronaves e pilotos inimigos.

No que compete aos ataques cibernéticos, verifica-se que o custo benefício de um ataque cibernético sempre precisa ser avaliado. Essa tarefa cabe à operadora, que dinamicamente replaneja a missão para manipular e minimizar a exposição a ameaças.

Ou seja, o sistema formado consegue planejar a missão, cumprir a missão e ainda se aparecer um risco dinâmico, ele consegue fazer um replanejamento. Surrealidade, os caras resolveram sistemas. Isso já é uma realidade.

Tanto no espectro eletromagnético, como na visão computacional, existe uma série de fatores importantes em processamento que fundamentalmente se utilizam da inteligência artificial para lidar com as ações dinâmicas. Obviamente esse tipo de processamento é conectado com o mundo, por meio de um *datalink* de planejamento.

Resumidamente, isso traz riscos e oportunidades bastante interessantes. Ver como se desenvolve uma retaliação no *ciberespaço*. Normalmente uma retaliação no mundo físico envolve um sujeito que dá um tiro e você retalia dando três tiros e por aí vai. Ou seja, a retaliação no mundo físico ocorre materializada por uma resposta com uma força um pouco mais alta. Só que no caso cibernético isso não está claro. O ataque mais possante e o homem responsável pelos impactos não estão muito claros.

Um exemplo típico de escalada de crise motivada por ataques cibernéticos repousa no caso de um drone norte-americano derrubado de forma cinética pelos iranianos. Como ninguém morreu, a resposta norte-americana se deu da mesma forma, ou seja, sem mortes do outro lado. Em suma, os norte-americanos fizeram um ataque cibernético contra o sistema de mísseis de cruzeiro iraniano. Em suma, a derrubada de um drone norte-americano foi capaz de escalar uma crise entre os EUA e o Irã.

Inclusive, essa é uma questão acadêmica. Como é que eu determino no mundo cibernético? Outra questão importante é que as operações de ataque cibernético demandam muito tempo de planejamento. Esse tipo de operação em países que têm o setor de guerra cibernética bem avançado, normalmente é precedido por meses de trabalhos, mas em alguns casos até anos.

Quero chamar a atenção para duas coisas. Eu tenho ataques, que por essência são ataques cibernéticos. Veja que coisa interessante, 46% dos provedores do Departamento de Defesa norte-americano tiveram problemas com materiais eletrônicos. Isso é uma coisa que a gente não faz no Brasil. Vamos reformar a *General Eletric* e a mesma não sofrerá uma intervenção em sua cadeia logística por parte das autoridades governamentais brasileiras. Isso é fundamental para a execução de uma estratégia.

Eu vou falar um caso interessante que ocorreu em 2012. Nessa época, 80% dos produtos da TELECOM eram compostos por componentes chineses. Uma crise com o governo chinês poderia causar uma grave paralisia na cadeia logística, assunto que

começou a causar terror no Brasil. Dessa forma, um programa foi elaborado com o intuito de proteger a cadeia de suprimento desses componentes eletrônicos.

Todavia, há uma característica fundamental no componente eletrônico, que é o seguinte: eu posso fazer 100 componentes e um somente estar adulterado. Da mesma forma que eu também posso colocar 100 computadores no Quartel General do Exército Brasileiro e somente um estar alterado. Como é que eu consigo pegar esse único computador que está adulterado? Eu não pego.

A única forma de você testar se há um componente adulterado é por meio de testes destrutivos. É o Cavalo de Tróia perfeito. Ou seja, a única forma de testar é realizar uma destruição. Vou dar um exemplo. Para você, isso aqui é um *chip* qualquer. É o tipo de coisa que está visível aos olhos de todos. Você pode ver que o *chip* possui somente 2,27 milímetros de largura. O mundo digital é completamente distinto do mundo físico. No mundo real, se eu realizo uma fricção num pequeno objeto, ele mexe um pouco, agora se a fricção for muito grande, ele mexe muito fiscamente. Ou seja, é previsível. Já no mundo digital é diferente, um único *bit* pode mudar 100% do comportamento do sistema. É aquele entra e sai que apaga tudo ou aquele *enter* que é dado que você lança um míssil balístico.

Essa dificuldade do mundo digital não é linear. Muitas vezes, a mudança de um único fio desse *chip,* faz com que o comportamento dele seja completamente mudado. Criar ou ativar um Cavalo de Tróia adormecido pouco custa, basta apertar a tecla *enter* de um computador.

Vamos supor que o Exército Brasileiro vai comprar computadores para o Gabinete do Comandante. Sabe-se que a primeira parte do Ordenador de Despesa é fazer uma tomada de preço, fazer uma licitação, abrir edital. Quanto tempo isso leva? Entre falar que vai comprar e ter comprado (90 a 120 dias). A contra inteligência do inimigo descobre que isso será comprado pelo Gabinete do Comando do Exército Brasileiro. Então, eles modificam o vídeo de computadores que serão comprados e inserem o vírus que eles quiserem. Preciso lembrar que o Exército Brasileiro vai comprar computadores que estavam zerados. A conclusão disso é que é um absurdo fazer compra de material para determinados departamentos estratégicos de um Estado por meio de licitação. Pergunta se o norte-americano faz licitação para a compra de computadores para departamentos estratégicos de um Estado? Se o norte-americano fizer uma compra nesses termos, ele vai constatar ineficiência na cadeia logística.

Vamos falar do transporte, que pode ser um *download* ou pode ser de fato um transporte. É o local onde as operações táticas encontram maior facilidade para atuarem. Isso é um crime de lesa pátria, mas ajudou todo o resto das outras pátrias, pois se trata de um grupo da NSE abrindo com cuidado roteadores da CISCO SYSTEMS e inserindo o que eles chamam de *Bicon Londres*.

Não tem bonzinho. Eu fui funcionário da MICROSOFT, da INTEL e da CISCO. Você vê o nível de cinismo. Esse pessoal tem algumas questões. A primeira questão é por que a gente não faz isso? Essa pergunta não irei responder. A segunda questão é razoável pensar e planejar a guerra eletrônica, a guerra cibernética e os sistemas autônomos de forma integrada? Sim, porque não dá mais para falar dessas coisas de forma estanque, tudo isso aí faz parte de uma mesma coisa só.

A guerra do futuro passa pela cibernética, pela eletrônica, etc. O Brasil está na hora de ter uma Estratégia de Guerra. Esse assunto é pouco explorado no Brasil. No entanto, deveria ser mais explorado para que o mesmo possa se proteger contra esse tipo de coisa.

E se um sistema autônomo matar um ser humano? Isso é absolutamente assimétrico. Se eu perco o sistema autônomo, não perco nada. Agora, uma vida humana é irrecuperável. Dessa forma, esse é o pensamento que deve ser considerado na elaboração de sistemas autônomos. Outro exemplo: O combate estabelecido entre um Drone e uma aeronave é simétrico? Parece ser mais ou menos simétrico. Daí eu estabeleço a seguinte pergunta: Como é que sabemos que aquela plataforma identifica se o alvo é amigo ou inimigo? Eu vou dizer que os norte-americanos querem nos empurrar o sistema deles.

3. Conclusões

Último ponto recai sobre a dependência tecnológica do Brasil. Não há nenhum sistema hoje no país, no mundo, que seja 100% isolado. Quem está mais próximo disso é o francês e o norte-americano. A China, por seu turno, está tentando por toda a força vencer o *windows* e a *intel*, mas não consegue. Entretanto, uma coisa está óbvia em todo o mundo: é preciso ter capacidades mínimas para não virar refém tecnológico. Na verdade, eu chamo de cativeiro tecnológico nas questões afetas aos sistemas autônomos. Quem garante que o sistema autônomo não se oporá a mim? Ninguém. Posso ser *hackeado*. Mais do que isso, ele pode, pelo fabricante ou pelo país de origem, se voltar contra você no último momento ou no momento em que você mais precisar.

Muito obrigado pela atenção!

O DOMÍNIO DA NARRATIVA NAS OPERAÇÕES DE INFORMAÇÃO E OS ATAQUES CIBERNÉTICOS

Tenente-Coronel Alexandre Santana Moreira*

1. Introdução

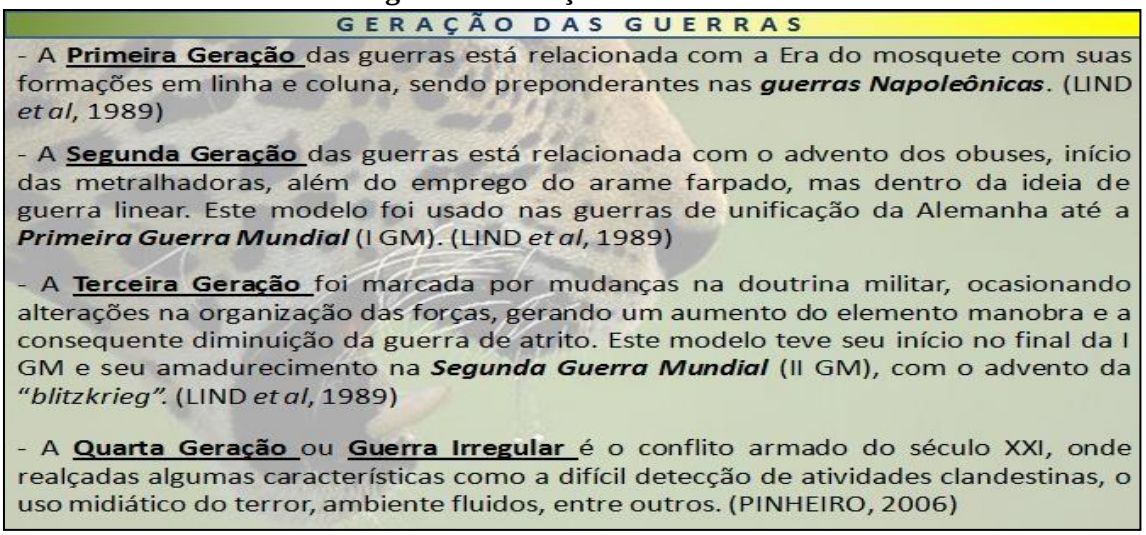
Bom dia.

É um prazer estar retornando a essa casa, onde tive a oportunidade de passar um tempo como instrutor. Aos companheiros que estou revendo, gostaria de deixar o meu abraço fraterno e a todos os senhores que não tive a oportunidade ainda de conhecer, deixo também meu abraço.

A proposta da apresentação procura dar ênfase no domínio da narrativa, nas operações de informação e nos ataques cibernéticos, aspectos que são cotidianos em nosso dia a dia. "Na guerra, a verdade é a primeira vítima". Essa frase elaborada por Ésquilo revela que os princípios e valores que a sociedade possui, incluso a verdade, não se sustentam numa guerra, pois a primeira coisa que morre é exatamente ela.

Para falar dessas coisas, é necessário relembrar uma teoria que trata sobre a geração das guerras: primeira geração da guerra (abarca a época das guerras napoleônicas); segunda geração da guerra (envolve o entorno da 1ª Guerra Mundial com as inovações da metralhadora, dos gases e outros); terceira geração da guerra (é a guerra de movimento, característica da 2ª Guerra Mundial); e quarta geração da guerra (é a guerra irregular, que vem desde o final do século XX e alcança o início do século XXI):

Figura 1 - Geração das Guerras



Fonte: o autor, 2019.

* Doutor em Ciências Militares e Comandante do 1º Batalhão de Comunicações de Selva.

A quarta geração da guerra antecede o que enfrentamos nos dias atuais. Os militares, em sua grande maioria, foram formados sob os auspícios da quarta geração da guerra (combate aos guerrilheiros). Contudo, o cenário evolui, cresce, caminha. Há uma teoria das ondas onde a humanidade cresce e evolui e quem está sempre sobre as ondas consegue auferir os maiores lucros.

Isso é algo natural e aí nós chegamos praticamente nos tempos atuais onde a revolução da informação vai despertar nas pessoas a necessidade da gestão do conhecimento, porque são tantas coisas e tanta informação que não sabemos o que fazer com elas. É necessário gerir, entender e tirar os ensinamentos para que possamos tomar uma determinada ação.

E aí entramos na guerra de quinta geração, onde a nanotecnologia, a biotecnologia e a guerra cibernética crescem e avultam de importância. É o ambiente que nos encontramos hoje. O desenho a seguir é para mostrar que além da profundidade da questão aeroespacial, há também o crescimento do espectro eletromagnético e da área cibernética nessa dimensão, sob o escopo da quinta geração das guerras:

Figura 2 - Ambiente Operacional Atual

Fonte: o autor, 2019.

A cibernética é algo que vem com bastante força e intensidade. Verifica-se, sobretudo, que é muito difícil achar o oponente num combate assimétrico. Normalmente ele conta com poucos meios, mas que são capazes de causar um estrago grande.

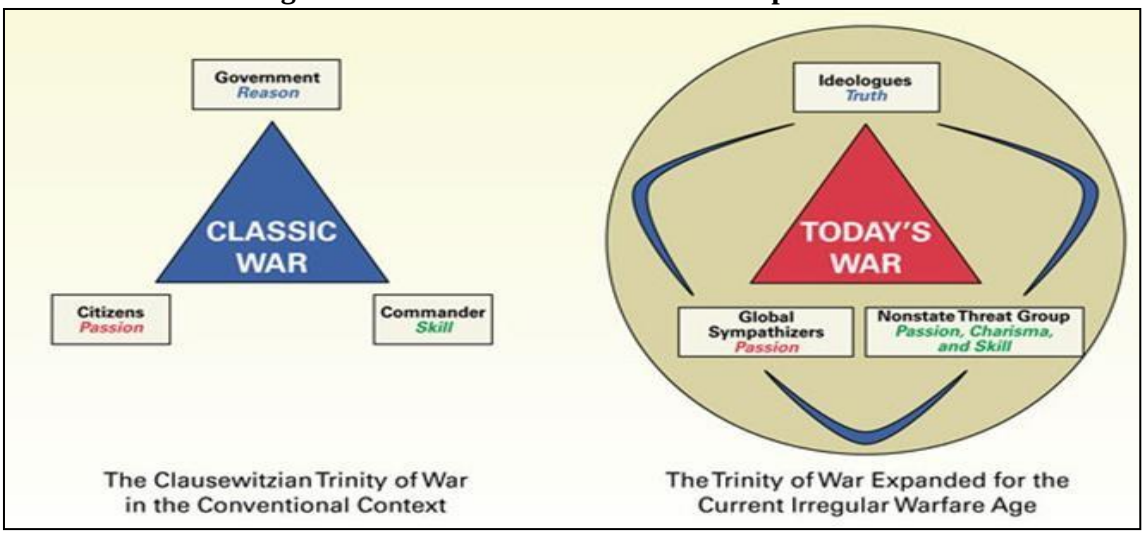
Diante dessa realidade, o Exército Brasileiro precisa contar com elementos aptos a essa nova realidade, algo de dificil execução nos dias atuais. Para que se tenha uma ideia, vários Exércitos do mundo já trabalham com essa linha de raciocínio.

O cenário atual é caracterizado pela ampla utilização das mídias e das redes sociais, pelo grande ativismo na *internet* e por muitas campanhas feitas para diversos fins

na *internet*. Dessa forma, chega-se às nossas manobras dentro dessa dimensão, as quais possuem grande dificuldade, haja vista que as mesmas tendem a serem mais fluidas, plurais, instantâneas, sempre com foco voltado na procura de oportunidades que podem aparecer. Nesse prisma, destaco que existem coisas que são praticamente antagônicas, mas para que eu possa ter intento, o ideal é que possamos buscar a efetividade desses principios e conceitos.

Clausewitz não morreu e a sua trindade continua existindo, apesar de muitos teóricos afirmarem que a trindade dele está evoluindo para uma nova trindade. A tríade *clausewitziana:* Governo - Cidadãos - Forças Armadas está sendo substituída pela tríade contemporânea: ideologias - simpatizantes globais - atores não estatais. Poderíamos dizer que é um duplo triângulo, com a coexistência de todos esses atores, que dependendo do momento e da atuação, funciona mais para um lado do que para outro e vice-versa. Em suma, a guerra não mudou, ela está mais complexa, pelo que se reflete na complexidade das operações, do raciocínio, do preparo e do planejamento:

Figura 3 - Trindade da Guerra Contemporânea



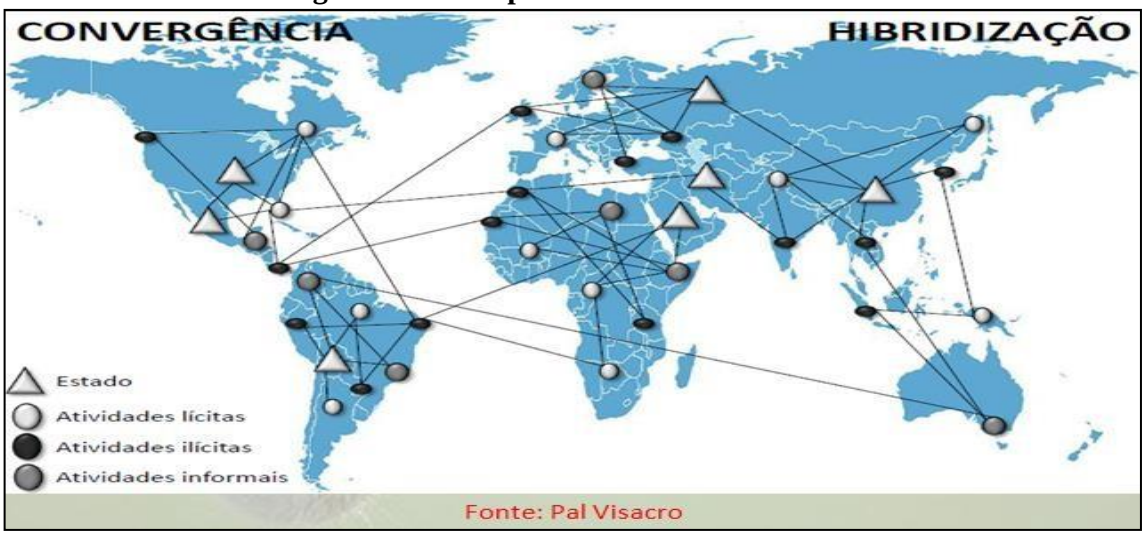
Fonte: o autor, 2019.

Antigamente, os objetivos eram muito fáceis, nos dias atuais a realidade não é assim. Hoje é difícil a compreensão de uma missão, pelo que também é difícil analisar e visualizar as suas consequências. Aí vem a importância da ECEME. Esta escola nos dá a ferramenta para entender uma área nebulosa onde ninguém consegue ver, mas aponta o caminho que deve ser seguido. Utilizando o método adequado, consegue-se visualizar uma linha de raciocínio. Pode não ser a melhor, mas é uma linha que vai atender em muito boas condições o meu problema.

É importante lembrar as falas do Coronel Visacro, o qual destaca que a complexidade hoje é de tal forma, que há uma convergência de interesses de atores

múltiplos, com origens e ideias diversificadas, mas que se juntam para cumprirem determinado objetivo. O que gera a guerra híbrida ou a hibridização dos conflitos atuais não é o narcotráfico. O narcotráfico tem diversos tipos de aliados: governo, políticos, sociedade mercantil, escolas, faculdades, etc. Por isso, não adianta somente focar em apenas um dos atores, porque os outros continuam em pé. Dessa forma, algumas operações nos fornecem a sensação de que as tropas parecem estar enxugando gêlo, porque se tira um traficante e aparece outro amanhã e por aí vai. Ou seja, não é só o traficante ou o bandido, não é só aquele inimigo, pelo contrário existem muito mais coisas envolvidas e o processo é muito mais complexo do que se pensa:

Figura 4 - A complexidade do mundo atual

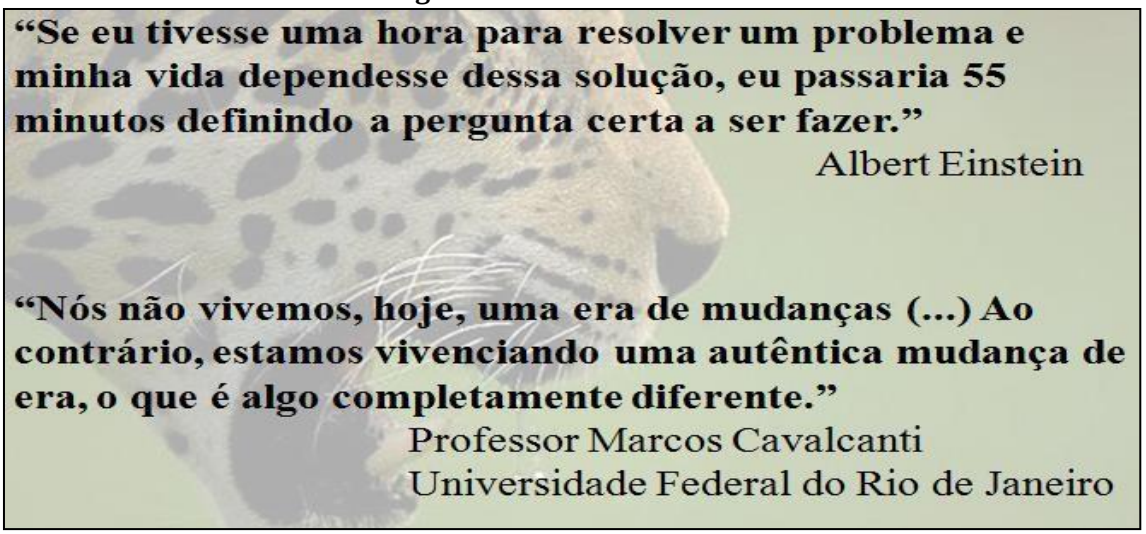


Fonte: o autor, 2019.

O conceito de insurgência criminal revela que há um predomínio da violência armada não estatal nos dias atuais, pois ela é organizada, endêmica e totalmente difusa. O aspecto importante a ser ressaltado é que o cumprimento da missão não fica restrito apenas a tomada de um morro. Isso não vai resolver o problema, se fosse assim o Rio de Janeiro já estaria com seu problema resolvido. Mas, efetivamente, o problema não é esse, ele é muito mais complexo que possamos imaginar.

"Fazer certo as coisas versus Fazer as coisas certas". Essa é uma frase famosa do General *Stanley McChrystal,* que não é só uma retórica, mas um jogo de palavras. Fazer certo as coisas é: cortar o cabelo, entrar em forma, pegar o armamento, entra em linha, sobe o morro, faz a patrulha, etc. Desse jeito, estamos fazendo certinho e não há o que questionar sobre isso, mas talvez não seja a coisa certa a ser feita. Porque a coisa certa a ser feita passa pela hibridização, passa pela convergência, passa por outros atores que talvez ampliem nosso campo de visão e atuação. E novamente essa Escola, com seus métodos, pode ajudar na superação desse desafio dando uma direção geral.

Figura 5 - Frases reflexivas



Fonte: o autor, 2019.

Qual é o problema do Rio de Janeiro? É tão complexo que eu tenho que passar muito tempo pensando e analisando, pois não é uma solução simples, na medida em que a mesma depende da opinião pública para dizer que o problema está resolvido. A opinião pública nunca esteve tão fortemente aliada com as tropas como nessa ultima operação e o problema de violência no Rio de Janeiro continua. Isso não é uma crítica a ninguém. Estou apenas querendo destacar que o problema é muito mais complexo do que se pode imaginar.

Estamos presenciando uma ruptura de paradigma, tais como algumas mudanças na sociedade, modelos e padrões consagrados ao longo do tempo se tornam obsoletos, determinados tipos de ações, de guerras e de conflitos já perderam a sua maneira de agir, seu *modus operandi*, etc.

2. Desenvolvimento

Esse preâmbulo foi utilizado para dar uma contextualização da narrativa, que é o objetivo de hoje. E o que isso tem a ver com a narrativa? A narrativa circula nesse ambiente complexo. De uma maneira geral, o brasileiro tem a mania de dizer se tal narrativa é de direita ou de esquerda, mas às vezes não é de direita e nem de esquerda. Não sabe nem o que é, mas quer perturbar o ambiente e nós temos que saber definir esses fatos novos porque rotulamos algumas vezes e achamos que os rótulos vão resolver o problema, mas nem sempre resolve.

Um exemplo típico disso é o responsável pelo ataque cibernético mais famoso do momento: o senhor *Glenn Greenwald*. Ele é de esquerda ou de direita? Talvez ele não seja nem de esquerda e nem de direita, mas tão somente um *hacker*. O que é um *hacker*?

O *hacker* é uma pessoa que ninguém vê, ninguém sabe se ele gosta disso ou daquilo, mas ele está interessado em outras coisas, principalmente no dinheiro e quem paga mais.

Numa narrativa, preciso saber quem fala, o que fala, como fala, quando, onde e o porquê disso ou daquilo. Ao lermos um artigo no jornal, normalmente o mesmo se torna uma verdade absoluta, entretanto está muito longe de ser uma verdade, quanto mais absoluta. E eu tenho que entender isso, pois uma narrativa é composta de elementos: o narrador, o personagem, o espaço, o tempo, o problema e a solução da questão.

Nessa perspectiva, preciso entender que nem sempre quem está escrevendo é o narrador, nem sempre o narrador é quem escreveu e nós muitas vezes confundimos porque o jornalista disse e nem sempre ele disse, ele pode estar contando a história de alguém. Isso precisa ser compreendido para que não coloquemos rótulo em aspectos que não representam a verdade. Há que se recordar que existe a figura do narrador participante, do narrador que observa de fora e do narrador que sabe de tudo que vai acontecer na história. E numa história, existe sempre a figura do protagonista e do antagonista.

Então, quando eu leio um artigo de jornal com todos esses aspectos presentes, preciso entender que aquele personagem possui uma máscara. De acordo com a minha história, aquele personagem praticamente mantém uma linha, o qual pode ser um personagem complexo em termos de sentimento de emoções, pode ser também do tipo caricata, pode ser de um tipo já conhecido, etc. Nessa moldura, temos que entender que o escritor direciona seu manuscrito para alguém, de acordo com um determinado tipo de personagem e se o jornalista quer colocar uma caricatura na autoridade, ele vai buscar características da caricatura que o encaixe, vai achar uma justificativa para tal atitude.

Fato é que às vezes temos esse sentimento de ler essas coisas e aquilo ser uma verdade. A complexidade do tema não está no que se fala, mas no que as pessoas entendem e normalmente elas se dão mal. Numa conversa de homem para homem, é natural que o outro olha para cima, para baixo, para o lado e a conversa continua e termina todo mundo feliz. Poxa, que legal! Ele conseguiu me ouvir. Já numa conversa entre homen e mulher, quando o homem olha para cima, a primeira coisa que uma mulher faz é preguntar o motivo que o homem está olhando para cima. Conversar com mulher é diferente, tem muito mais coisa envolvida: gestos, atos, atitudes, olhares, etc.

Ou seja, a comunicação não é uma coisa simples de ser feita, apesar de todo mundo achar que sabe falar bem e sabe se comunicar bem, lembro que a pessoa que recebe a comunicação possui fundamentos antropológicos, sociológicos, psicológicos, filosóficos,

distintos da pessoa que emite a comunicação. Então, a pessoa que recebe, absorve as informações de acordo com seu filtro individual:

Figura 6 - Fundamentos da Comunicação

Fonte: o autor, 2019.

De antemão, eu tenho que saber quem é o autor, qual a filosofia dele, para quem ele escreveu e quando for ler, preciso tirar dali tudo aquilo que ele fez e concluir sobre qual a idéia que ele quis passar. Portanto, eu não leio mais livros, eu leio autores, eu leio princípios, eu leio fundamentos. Eu extraio as mensagens sem que aquilo seja uma verdade eterna. Ela é uma mensagem do fulano para o ciclano, de acordo com espaço e tempo e isso muda a maneira de ler os artigos e outras coisas.

A comunicação é influenciada por uma série de coisas, tais como: pela linguagem verbal, pela linguagem não verbal, pela percepção, pela redundância, pela forma de falar e pelo que vestimos. Existem reações involuntárias do comunicador que precisam ser controladas. Às vezes, uma pessoa percebe que a outra não gostou, simplesmente pelas reações involuntárias que o comunicador realiza. De toda sorte, cumpre salientar que 35% de qualquer conversa correspondem às palavras faladas e os outros 65% restantes correspondem aos gestos e articulações. Uma pessoa que for para a China hoje, sem falar um pingo de chinês, pode passar um mês lá tranquilo. Basta apontar o que deseja comer e por aí vai. Eu tenho que entender a expressão facial e sempre devo tomar muito cuidado com isso. Dessa forma, ressalto a importância da empatia, que dá uma sintonia muito forte para quem está nesse processo.

Alguém se recorda do debate político ocorrido em 2010? O que foi falado? Quem disse o que? Ninguém lembra. A única coisa que nós lembramos é o caráter. Por que a então candidata Marina está muito calada, por que aquele ali está muito caladinho, por que a ex-presidente Dilma está agindo dessa forma? Ninguém lembra. As pessoas se

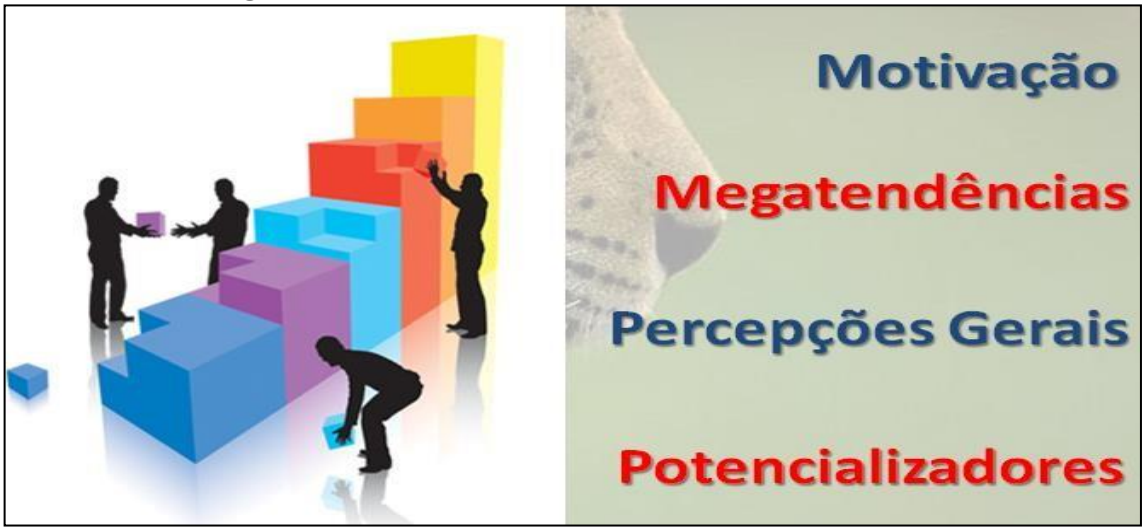
recordam do contexto geral, principalmente do caráter das personalidades que estavam presentes, o que não é exatamente a comunicação que foi feita naquela situação.

Figura 7 - Elementos não verbais do caráter

Fonte: o autor, 2019.

Em suma, comunicação e atitude são totalmente diferentes, pois a comunicação é o que é percebido pela outra pessoa, de acordo com as características sociais, com a predisposição que ela já tem com o tema, com a cultura e de acordo com o contexto que está inserido. Assim, para que determinado grupo seja alcançado, é necessário adotar outra verbalização, outra contextualização e talvez até outra postura para atingir outro grupo. Torna-se necessário tomar muito cuidado e analisar o terreno que será trafegado. Mesmo que a intenção seja muito boa, a comunicação pode ser muito ruim e prejudicar a ideia que se está querendo transmitir.

Figura 8 - Elementos influenciadores da comunicação



Fonte: o autor, 2019.

A comunicação que se dá por gestos, palavras, símbolos, também é afetada e/ou

influenciada por aspectos como: motivações, tendências, percepções e potencializadores da minha comunicação e da minha narrativa.

Qual é a motivação que eu preciso ter? Independente do motivo há certas tendências que estão em voga nos dias atuais. Se for querer falar de exercício militar, que não está na moda, talvez não tenha alguém que queira transmitir essa proposta. Mas, se for falar do combate à corrupção, o jornalista na mesma hora irá aceitar essa proposta, porque esse assunto é uma tendência nos dias atuais. É com base nesse contexto que procuro fazer a minha narrativa, já direcionando a mesma para as megatendências dos dias atuais. Assim, não vou falar de formaturas, vou dizer que combatemos a corrupção nos quartéis, inclusive tem uma formatura hoje, que é o contexto que eu tenho.

As percepções gerais estão de acordo com a idéia que eu quero passar. A percepção é materializada de acordo com os critérios que temos de domínio, sensualidade, positividade, força, segurança, código de cores. Por que o símbolo do *MC Donalds* é vermelho? Por que em sua parte interna é laranja? Existe um estudo de códigos de cores para que seja assim. Por que dentro do hospital é branco e não preto? Por que uma discoteca é preta e não é branca? Tem um estudo do código de cores que revela que uma determinada cor fará isso, outra cor poderá produzir aquilo e por aí vai.

E existem os potencializadores. O modo de ler, de ver, de falar, de agir (se estou sendo muito enérgico ou não, se o dedo está sendo apontado ou não, se levanto a mão ou não, se eu sou mais quieto ou não, se a mão está para trás ou não) pode potencializar a comunicação. Não pelo acaso, as autoridades são bastante treinadas, uma vez que o comportamento das mesmas pode potencializar a mensagem que pretende transmitir.

O que é notícia? Os militares não estão habituados a isso. Exemplo: se o cachorro morde o homem ou se o homem morde o cachorro, isso não é notícia. Mas, se o homem tivesse pagando o cachorro para realizar seus favores sexuais, isso se tornaria uma noticia. Mas, para ser uma notícia de primeira página, para ser machete, o cachorro teria de ser menor de idade e o homem deveria ter um cargo importante no governo. Essas definições fazem parte de uma pesquisa elaborada pela Folha de São Paulo. Ou seja, a notícia carrega consigo interesses diversos. Por que determinada notícia que a gente fala não é transmitida? É interessante para quem? Para qual grupo?

A notícia tem que ter seu ineditismo, a probabilidade daquilo acontecer, o apelo, a empatia. Uma formatura no quartel virar notícia é difícil, mas quando a mesma se constitui numa atividade para iniciar uma operação ou para homenagear alguém, então a mesma passa a ser um pequeno detalhe de uma notícia bem mais ampla.

Precisamos entender como trabalha o jornalista. Ele é um profissional que via de regra, está em busca da verdade, tem formação humanista, possui grande sensibilidade, é jovem, competitivo, busca a verdade, é curioso por excelência, generalista, representa a sociedade e isso tem que estar claro. Mas, se ele vai publicar a verdade ou não, isso já é outra história e temos que entender que o jornalista integra um conjunto muito maior que contempla um corpo de trabalhadores, jornalistas e outros que trabalham na área:

Figura 9 - O corpo jornalístico

Fonte: o autor, 2019.

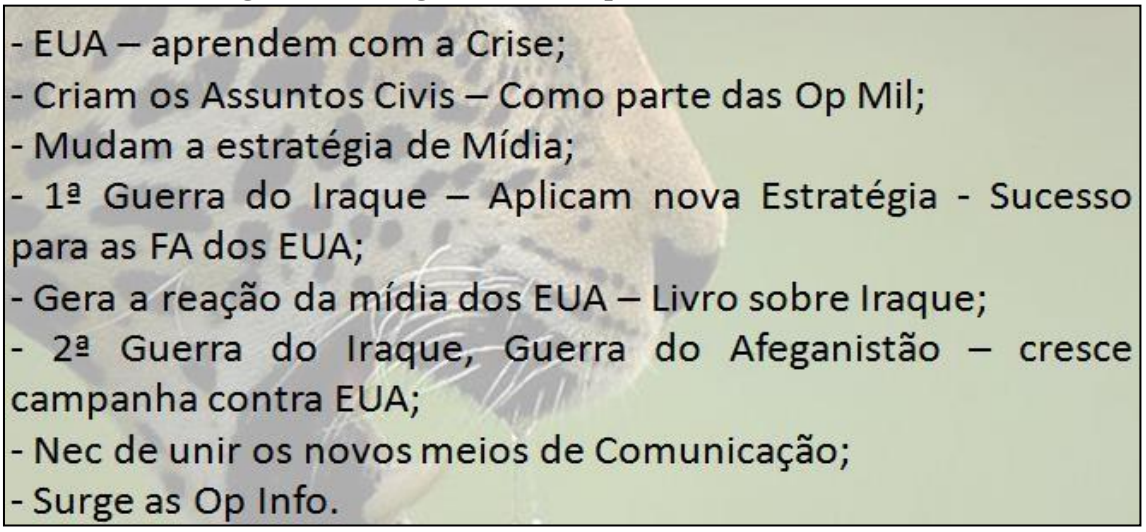
Diante disso, quando vou comunicar algo, tenho que entender o contexto, há toda uma narrativa por trás. Se ele não publicou o que eu falei, provavelmente não publicou porque não tem interesse. Eu tenho que entender qual é o jornalista, qual é a empresa, quem vai veicular aquela informação, etc.

Hoje, para enfrentar o combate de quinta geração, com elementos que trabalham na quinta dimensão na área cibernética, fica muito difícil trabalhar com esse pessoal. Fato é que todo mundo está precisando se reinventar. Se eu estou falando com a mídia tradicional, tudo o que foi falado aqui continua valendo. Porém, se vou combater o pessoal da guerra de quinta geração, a conversa é outra.

A necessidade de trabalhar a comunicação vem desde a Guerra Fria. Na Guerra do Vietnã, os norte-americanos perderam a sua opnião pública e eles tiveram que se reinventar. Na primeira guerra do Iraque, os militares norte-americanos transformaram a relação que tinham com a sociedade e conquistaram o apoio da mesma, de tal forma que praticamente não houve críticas às ações militares. Um dos aprendizados do Exército dos EUA colidos na Guerra do Vietña e posto em prática na Guerra do Iraque foi inserir o jornalista dentro do Pelotão, para que pudesse gerar uma sintonia entre ele e as tropas de primeiro escalão. Com a evolução das guerras e dos conflitos, os EUA viram que é

necessário unir mais coisas (além das operações psicológicas e da comunicação social). Enquadram-se nesse universo a *internet*, a guerra eletrônica, fenômenos que provocaram o surgimento das operações de informação e o seu campo informacional:

Figura 10 - Surgimento das Operações de Informação



Fonte: o autor, 2019.

Sob uma perspectiva lógica, há os conteúdos, o fluxo, a qualidade, a automação e o que vai gerar que eu tenho uma estrutura, tanto ofensiva, quanto defensiva de atuação. A figura abaixo apresenta os países que desenvolvem operações de informação, com seus respectivos níveis: nível político, estratégico, operacional e tático:

Figura 11 - Surgimento das Operações de Informação

País	Tipo de documento	Atualizações	Nível de PIi
Bélgica	Doutrina Conjunta	2009	Operacional e Tático
Canadá	Política Nacional e Doutrina Conjunta	1998, 2004 e 2009	Político, Operacional e Tático
Alemanha	Doutrina Conjunta	2002 e 2005	Político, Estratégico e Operacional
Holanda	Política Nacional	2001	Político
Noruega	Conceitos e Livro Branco	2002 e 2003	Político
Suécia	Doutrina Conjunta	2004	Estratégico e Operacional
Reino Unido	Doutrina Conjunta	2002, 2006 e 2009	Político, Operacional e Tático
Estados Unidos	Política Nacional, Doutrina Conjunta e Livro Branco	1996, 1998, 2002, 2003, 2006, 2012 e 2013	Político, Estratégico, Operacional e Tático
OTAN	Política Nacional e Doutrina Conjunta	2002 e 2009	Político, Estratégico e Operacional
UE	Conceitos	2003	Político
Brasil	**Doutrina EB**	**2014**	**Tático**

Fonte: o autor, 2019.

Há uma publicação da *Military Review* que afirma que a opinião pública é o centro de gravidade nas operações de informação. Porém, essa não é uma verdade irresoluta em si. Por definição, as operações de informação juntam, coordenam e direcionam as ações em campo. Como o General Richard disse: "as operações de informação não irão mandar na Comunicação Social e nem no CCOMSEX". Lembrando que isso foi devido aos vários

problemas em guerras passadas. Os norte-americanos entendem que as operações de informação conjugam as capacidades no sentido de direcionar os esforços numa campanha. O foco das operações de informação é obter a superioridade de informações, conforme a afigura abaixo:

Figura 12 - Foco das Operações de Informação

Fonte: o autor, 2019.

A comunicação social é uma ferramenta que trabalha com as percepções. Entrementes, tem a ver com a reputação e com a imagem. O relacionamento com a mídia precisa ser amistoso e precisa tomar os devidos cuidados. Essa figura abaixo mostra que uma foto dessa não comunica bem, porque tem gente olhando para baixo, olhando para o outro lado, etc. Então, tenho que tomar cuidado com o relacionamento com a mídia e com as mídias sociais, pois as mesmas crescem em importância.

Figura 13 - Cuidados com a Comunicação Social

Fonte: o autor, 2019.

No tocante às operações psicológicas, relembro que numa guerra a primeira vítima é a verdade. Existem atividades que estão abaixo da linha da ética em todo o mundo, gente

que trabalha com desinformação, boato, propaganda subliminar e outras coisas mais. É necessário ter cuidado com o que está escrito. Ações psicológicas e guerras psicológicas são coisas que naturalmente existem no mundo.

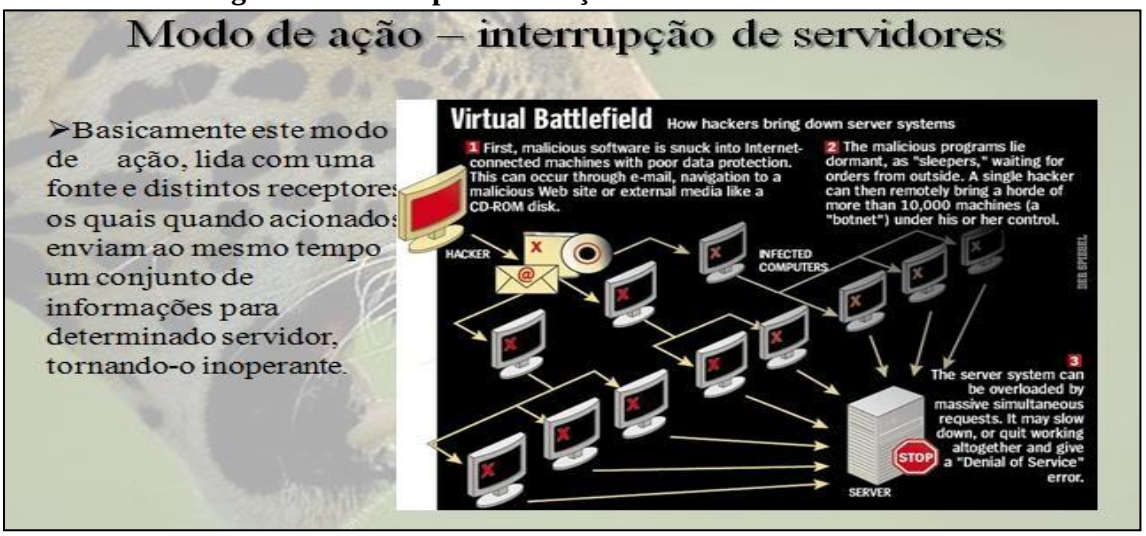
Figura 14 - Operações psicológicas e a linha da ética

Fonte: o autor, 2019.

A guerra eletrônica realiza suas atividades naturais do expectro (ouve o que se fala e capta o que os instrumentos falam) e por meio delas, geram conhecimento. Suas ações mais comuns são: obtenção de dados, localização, ataque e proteção. A inteligência, por seu turno, também não é diferente, pois ela trabalha com muitas coisas que nós não vemos para gerar adequada segurança.

A guerra cibernética já é realidade. A história já registra casos de ataques cibernéticos. A figura a seguir exemplifica um modo de atuação da guerra cibernética:

Figura 15 - Exemplo de atuação da Guerra Cibernética



Fonte: o autor, 2019.

Esse é um tipo de ataque por negação de serviço. Como exemplo, a negação de serviço é quando todo mundo em pé no auditório não conseguindo sair do mesmo, ou

seja, é muita gente tentando acessar em um único meio e o mesmo trava. Recordo o caso hitórico número um de 2007, ocorrido na Estônia, de onde gerou o manual TALLINN, que é a bíblia da cibernética.

3. Conclusões

Para que se tenha o domínio da narrativa nas operações de informação, torna-se necessário o entendimento dos princípios da narrativa e que os mesmos compõem as capacidades relacionadas à informação (CRI), no contexto das operações de informação. Ou seja, para que se obtenha êxito, é necessária a definição da direção geral, para que a comunicação social, a inteligência, a guerra eletrônica e a cibernética possam contribuir no esforço geral.

No Brasil, essas ações basicamente são desencadeadas no nível tático, mas nos outros países é possível verificar a ocorrência dessas ações nos níveis político, estratégico e operacional. A provocação que ficou foi: Quem faz isso hoje no nosso país nos níveis político, estratégico e operacional?

Não se deve esquecer que no mundo hibrido, onde uma solução simples não existe, onde um amigo não é tão amigo, onde o inimigo não é tão inimigo, onde o presidente ou ditador da Síria pode ser amigo de uma nação num ano e no outro não ser mais. A volatilidade e a mudança cada vez se fazem mais presentes atualmente.

Lembram-se do General *Stanley MCChrystal*? "Cuidado para nós não fazermos certo as coisas, temos que busca fazer a coisa certa". Essa perspectiva semeia as bases necessárias para a condução do planejamento conceitual para as operações de informação.

Termino a minha apresentação fazendo uma provocação junto à platéia. *Glenn Greenwald* é de esquerda ou de direita? O depoimento que ele deu ao Fantástico (programa jornalístico da Rede Globo de televisão) descreve que foi divulgada apenas uma pequena parte do conjunto de informações.

Ele, como ativista *Hacker* vai se aliar a quem quiser se aliar com ele. Dessa feita, destaco ratifico que um *Hacker* não tem partido, mas tão somente interesses, os quais irão evoluir de acordo com a situação e num mundo altamente complexo, essas coisas variam rapidamente.

Muito obrigado pela atenção!

O DOMÍNIO DA NARRATIVA NA MANUTENÇÃO DO PODER AEROESPACIAL

Brigadeiro Pedro Arthur Linhares Lima*

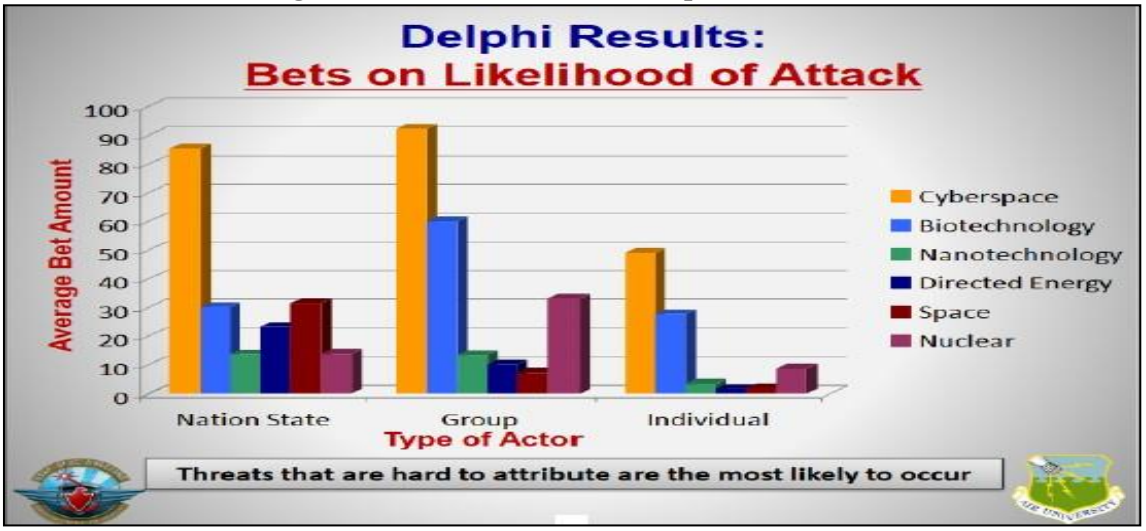
1. Introdução

Bom dia a todos.

É uma satisfação grande estar na Escola de Comando e Estado-Maior do Exército (ECEME), pelo que agradeço ao Comandante desta Escola e à comissão organizadora por ter feito esse convite.

Dentro desse contexto, a minha apresentação versará sobre o domínio da narrativa nas Operações de Informação e os ataques cibernéticos, com suas influências no poder aeroespacial. Sempre gosto de começar chamando atenção para o que vamos falar. Esse gráfico representa a probabilidade dos tipos de ataques no futuro:

Figura 1 - Probabilidade de ataques no futuro



Fonte: o autor, 2019.

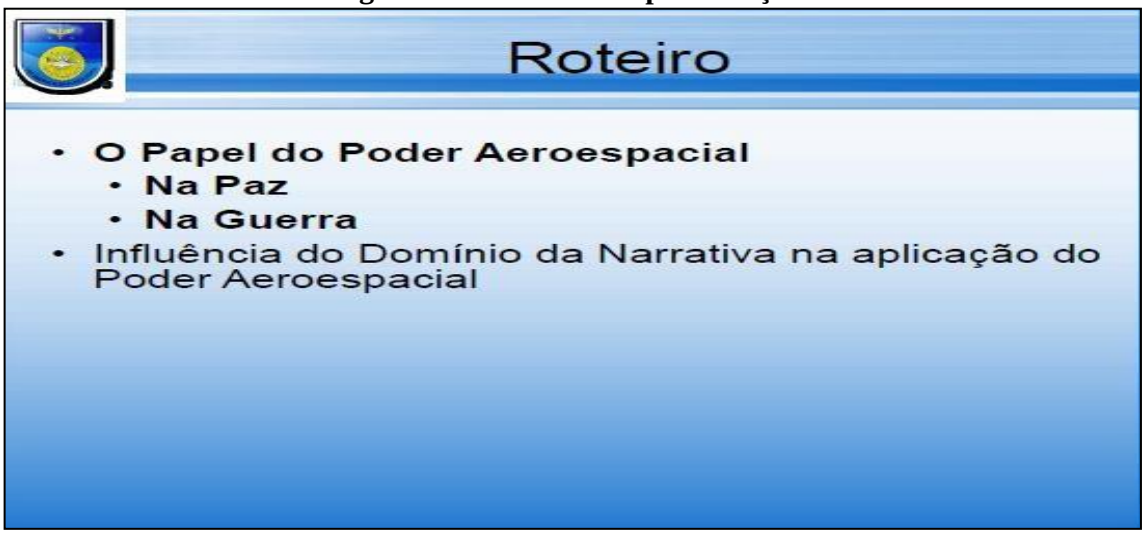
Verificam-se ataques nas seguintes áreas: cibernética, espacial, biotecnologia, nanotecnologia, nuclear e energia. Independentemente do tipo de ator (nação, grupos ou individual), percebe-se que em todas elas o ataque cibernético é o preferido. Nas nações, nota-se maior possibilidade do ataque proveniente do espaço, proveniente da parte nuclear (bastante utilizada por grupos e pouco utilizada por indivíduos). Se você pode utilizar todos esses aspectos para conseguir alcançar seus objetivos, seja ele qual for (individual, grupo ou nação), torna-se uma vantagem para o atacante, na medida em que o mesmo pode utilizar todo esse potencial.

---

* Doutor em Engenharia de Produção.

E o ataque desencadeado contra Estônia? Foi a Russia? Foram os nacionalistas? Aquele ataque foi patrocinado pelo governo? Não foi? Fato é que aconteceu e não se conseguiu até hoje ter uma atribuição. E esse tipo de ataque é o que a sociedade está acostumada a presenciar em todos os momentos. E como as Forças Armadas estão lidando com essa nova realidade? A resposta para essa nova realidade é muito mais complexa e interfere diretamente nas missões militares. Assim, o objetivo desta apresentação é identificar a importância do domínio da narrativa para a manutenção do poder aeroespacial. E para isso, vamos seguir o roteiro abaixo especificado:

Figura 2 - Sumário da apresentação



Fonte: o autor, 2019.

2. Desenvolvimento

Diante do exposto, torna-se importante conhecer o papel do poder aeroespacial, tanto em tempos de paz quanto em tempos de guerra, para facilitar na compreensão do domínio da narrativa e sua aplicação no poder aeroespacial.

A missão da Força Aérea Brasileira é manter a soberania do espaço aéreo brasileiro e integrar o território nacional, com vistas à defesa da pátria. Cumpre destacar a missão voltada para a manutenção da soberania do espaço aéreo brasileiro, pois se trata de uma missão com vertente muito importante tanto em tempos de paz, como em tempos de guerra, mas principalmente em tempos de guerra.

É importante mais uma vez relembrar que com relação ao controle do espaço aéreo brasileiro, a Força Aérea Brasileira é uma das únicas do mundo que realiza este tipo de missão. E para tanto, apoia-se numa infraestrutura comum com o setor civil. Em síntese, as mesmas tecnologias são utilizadas para o controle aéreo civil e para o controle aéreo militar.

Figura 3 - Controle do espaço aéreo

Fonte: o autor, 2019.

Ela possui uma vantagem. Por exemplo, a sociedade tem que ficar sempre se questionando sobre o que aconteceu nos atentados ocorridos em onze de setembro de 2001 nos Estados Unidos da América (EUA). Recordo que os norte-americanos têm uma infraestrutura aérea destinada para área civil e outra infraestrutura aérea voltada somente para a área militar, pelo que gera tratamentos distintos de sinais. Isso traz vantagens econômicas, mas também traz uma grande desvantagem em termos operacionais. Ou seja, se nos EUA os dois sistemas (civil e militar) estivesse unificados (um sistema apenas), com certeza as informações seriam tratadas da mesma forma com que nós tratamos aqui, o que reduziria as chances da ocorrência de tais ataques.

Destaco que o cenário internacional vem se tornando cada vez mais complexo. Até pouco tempo atrás, o sisetma internacional tinha em torno de 192 nações, que estavam sob a conjuntura do velho paradigma. O cenário de oposição e crise se limitava a nação *versus* nação.

A guerra de quarta geração inseriu novos incrementos, modificando a ordem internacional até então existente e trasnformando-a em novo paradigma (grupos de interesse - há mais de dez mil no mundo). Houve recentemente um ataque a um grupo de interesse, onde foi identificado e destruido um centro de defesa cibernético de um determinado grupo (*Hamas*). Esse grupo vinha causando uma série de problemas, não somente para Israel, mas para vários países do mundo. Em suma, o centro de defesa cibernético do grupo *Hamas* que foi detruído cinéticamente, representa apenas um dos mais de dez mil grupos de interesse existentes ao redor do globo nos dias atuais.

Os grupos de interesse começam a atuar nesse cenário, a favor ou não, sendo

orquestrado ou não por nações ou Estados, o que torna o processo de atribuição de responsabilidades muito mais complexo e difícil. O paradigma que está emergindo, e isso é fácil de perceber, é caracterizado pela facilidade com que as pessoas em geral podem causar danos. Ou seja, qualquer pessoa, qualquer criança, em qualquer lugar pode entrar na *internet* e baixar determinado *software* e inadivertidamente ou não, derrubar sistemas ou causar qualquer tipo de dano para uma empresa, para uma nação, etc.

Em outras palavras, estamos falando de indivíduos que podem causar danos, uma vez que a ferramenta necessária para a condução de tais ataques está disponível no mercado e ao alcance de qualquer pessoa. O planeta possui oito bilhões de almas inteligentes e isso aumenta a complexidade do nosso ambiente. Não estou considerando os agentes inteligentes, que são máquinas que podem fazer uma série de coisas, como os ataques de negação de serviço. Diante dessa realidade, se algumas pessoas não quiserem que esse sistema fique no ar, torna-se quase impossível a manutenção de um sistema desses no ar ou em operação. Ou seja, a gente está sempre um passo atrás, sempre reagindo.

Isso torna o ambiente que as Forças Armadas operam muito mais complexo. Voltando para o exemplo de controle do espaço aéreo tanto para o setor civil, quanto para o setor militar. No ambiente civíl de controle de tráfego aéreo é normal a realização de centenas de milhares de vôos com uma precisão cirúrgica. A comprovação disso repousa num episódio em que dois aviões da empresa GOL quase se chocaram. Bastou uma intefrência no sistema dos equipamentos de bordo e de auxílio à navegação, para os aviões quase se chocarem e irem ao solo. Ou seja, uma simples interferência em um sistema desses pode causar um sério acidente e não estou falando de um ataque de negação de serviço. Se o sistema de controle do espaço aéreo for derrubado, o mesmo pode ser controlado manualmente, como aconteceu.

Há possibilidade de controlar o problema se você não tiver a confiabilidade necessária das informações que você está recebendo. Um exemplo repousa no caso em que Israel entrou com aeronaves militares no espaço aéreo sírio, fizeram os ataques que tinham que fazer após a ação, as mesmas voltaram ilesas para Israel. O mais notório disso é que o controle de espaço aéreo sírio não detectou as aeronaves israelenses, apenas ficou olhando o céu de brigadeiro. Fato é que houve uma inteferência nos equipamentos sírios.

A figura a seguir apresenta a estrutura militar de guerra, que para ser acionada, deve haver algum fato que motivou a declaração de guerra por parte do país ou a reação à uma ação E para isso, essa estrutura é montada. Mas ela não é montada hoje e está

pronta amanhã. Sabemos que temos um tempo de reação para nomear o Comandante do Teatro de Operações, um tempo para identificar quais são as Forças Componentes que irão participar dessa atuação, do Teatro de Operações propriamente dito. Nós temos que mobilizar esse efetivo.

Figura 4 - Estrutura Militar de Guerra

Fonte: o autor, 2019.

Ou seja, estamos falando de vários dias, na melhor das hipóteses, para que nós possamos entrar com uma estrutura militar de guerra e começar a cumprir a missão atribuída. O problema é que nesse período o país não pode ficar parado esperando a mobilização.

Existe um comando conjunto ativado desde os tempos de paz e que funciona 24 horas por dia, há vários anos. Trata-se do Comando de Operações Especiais (COMAE), que realiza o monitoramento de todo o espaço aéreo brasileiro. Se alguém faz alguma coisa que não está prevista, há uma reação imediata. Dessa forma, o COMAE tem essa missão de dar a pronta resposta necessária, da mesma forma que realiza também o controle do espaço aéreo. Ou seja, todos os radares trabalham sob a égide do COMAE.

O aspecto crítico de sua pronta resposta e a confiabilidade das informações advindas do COMAE para que a Força Terrestre possa bem cumprir a sua missão torna o poder aeroespacial importante tanto nos tempos de paz quanto nos tempos de guerra. Dessa forma, ressalto a importância do dominio da narrativa nos ataques cibernéticos e nas operações de informações para que o país possa utilizar seu poder aeroespacial de forma soberana. Uma vez que o país consiga utilizar seu poder aeroespacial e seu controle de espaço aéreo de forma soberana, as outras Forças conseguirão cumprir suas missões sem muito atrito.

Os radares emitem um sinal e quando esse sinal encontra uma aeronave, esse pulso é refletido de volta e captado. É dessa forma que se consegue identificar um avião. Isso tudo é transformado em sinais de computador, os quais passam a ser analisados. A figura a seguir exemplifica o funcionam desses radares:

Figura 5 - Controlde do espaço aéreo

Fonte: o autor, 2019.

Isto posto, há duas alternativas para simular um "céu de brigadeiro". A primeira é enviar os pulsos não refletidos para outro local e a outra alternativa é anular o sinal, mas independente de qual seja a tática aplicada, esses radares vão transmitir essa informação de forma digital.

Os sinais que são transmitidos podem ser iterceptados e modificados, pelo que denota o caráter paradoxal dos radares. Se por um lado, os radares possuem grande importância, por outro lado os mesmos representam grande fragilidade no controle do espaço aéreo, aspecto que vai se refletir na supremacia aérea do nosso país. No Brasil, há centena de radares espalhados pelo território nacional, os quais são destinados exatamente para fazer o monitoramento do espaço aéreo brasileiro, tanto em tempos de paz, como em tempos de guerra.

A figura a seguir é um exemplo de uma linha de código que derrubou o tráfego aéreo inglês por uma hora. A Inglaterra é um país com a extensão territorial pequena, quando comparado ao Brasil, mas com uma quantidade de vôos enorme. Imaginem o estrago e o caos que causou a paralisação do controle de tráfego aéreo parado uma hora na Inglaterra. Agora, imaginem essa mesma situação se o país estivesse enfrentando uma guerra:

Figura 6 - Caso inglês

Fonte: o autor, 2019.

Uma simulação acompanha o que está acontecendo, na realidade o que estava planejado para acontecer. Cabe ressaltar que todo o planejamento de guerra é feito usando uma rede de computadores, *softwares*, sinais de radar, sinais de satélite, etc. Ou seja, essa é a complexidade das nossas operações, as quais utilizam todo esse manancial tecnológico para cumprirem suas missões. Qualquer interferência nesse processo vai causar distúrbio e problemas na aplicação quando nós estivermos no campo de batalha.

Esse exemplo consiste nas aeronaves francesas que não conseguiram decolar por causa de um vírus. Isso é uma vulnerabilidade do F16, uma aeronave altamente tecnológica e com grande capacidade militar. Sobretudo, ela é vulnerável aos ataques cibernéticos.

Figura 7 - Caso francês

Fonte: o autor, 2019.

3. Conclusões

O espaço cibernético faz parte da nossa vida, do nosso dia a dia. Esse espaço cibernético é um novo domínio da guerra, que perpassa toda Força Terrestre, toda Força Maritima, toda Força Aérea e todo o espaço.

Figura 8 - Escopo do espaço cibernético

Fonte: o autor, 2019.

Já conseguiram imaginar se um satélite deixa de enviar sinal? Já fizeram um exercício? Se um GPS parar de receber sinais o que acontece em nossas vidas? Não estou falando de guerra, estou apenas ressaltando aspectos do nosso dia a dia. A quantidade de serviços que não vamos conseguir utilizar, simplesmente porque um sinal de satélite parou de enviar informações é gigantesca.

Se nós pararmos uns cinco minutos fazendo esse exercício, nós iremos verificar o quanto dependentes somos do espaço. E nesse sentido, o espaço nos preocupa porque assim como o Exército Brasileiro ficou incumbido de desenvolver a cibernética, a Força Aérea Brasileira ficou incumbida de desenvolver a parte espacial, a qual está baseada em computadores, redes e sinais. Ou seja, aspecto muito mais vulnerável do que a Força Aérea e a Força Terrestre. Mal ou bem, a Força Terrestre tem como se mover para cumprir a missão. Mal ou bem, a Força Aérea, se não for invadida por nenhum vírus, consegue cumprir a sua missão. Mas a parte espacial é muito mais vulnerável, pois fica totalmente comprometida.

Essa é uma nova área importantíssima, que está totalmente baseada em redes e computadores. Imaginem se todo esse potencial for direcionado de uma forma para construir uma narrativa e atingir determinado objetivo. Recentemente, nós tivemos a utilização das mídias sociais para enfraquecer psicologicamente o inimigo.

Então, essa interferência afeta diretamente o psicológico do nosso pessoal, uma vez que consegue enfraquecer a vontade de guerrear. Há vários exemplos desse tipo de

interferência, pelo que acaba complicando não só as Forças Armadas, mas também a sociedade em geral. As eleições norte-americanas são um exemplo clássico da interferência das mídias sociais no processo eleitoral.

Muito obrigado a todos!

CENTRO DE DEFESA CIBERNÉTICA

General de Brigada Alan Denilson Lima Costa*

1. Introdução

Boa tarde senhoras e senhores.

É um prazer para o Centro de Defesa Cibernética (CDCiber) poder participar desse evento tão relevante para o momento que a sociedade vive há alguns anos. Quando íamos fazer uma apresentação em eventos realizados em outras instituições para falar sobre cibernética, passávamos muito tempo na introdução, cerca de 10 minutos, para explicar a importância do setor cibernético para o país e para as Forças Armadas. E para a nossa alegria, hoje não precisamos perder mais tempo porque o tema é muito atual, todos os dias o assunto faz parte da pauta do Jornal Nacional, da imprensa nacional e internacional. Se abrirmos as resenhas diárias que o Centro de Defesa Cibernética elabora, iremos constatar que a quantidade de fatos cibernéticos que estão acontecendo no mundo diariamente é imensa. Em vista dessa realidade, torna-se importante selecionar criteriosamente os casos para colocar na resenha.

O que nos dá muito orgulho para transmitir é o fato de que as Forças Armadas Brasileiras saíram da estaca zero a dez anos atrás e hoje estão em outro patamar. O setor cibernético de defesa evoluiu muito em dez anos. Poderíamos ter caminhado mais, mas a trajetória que foi percorrida ao longo desses 10 anos coloca o Brasil e as Forças Armadas Brasileiras numa situação diferenciada, principalmente aqui no hemisfério sul. Dessa feita, o propósito dessa apresentação é mostrar o Centro de Defesa Cibernética (CDCiber) e suas capacidades. O CDCiber é uma organização militar diretamente subordinada ao Comando de Defesa Cibernética (ComDCiber), pelo que lhe confere o *status* de braço operacional do Com DCiber.

Será falado sobre as situações de emprego, missão, organização e os princípios de atuação do CDCiber. Na sequência, será tratado sobre as áreas funcionais, que são aquelas que dão vida ao CDCiber. Na verdade, as áreas funcionais caracterizam a atividade operativa da defesa cibernética. Em prosseguimento, serão feitas algumas considerações acerca da atuação do CDCiber, nas formas sistemática e episódica, e na parte final será apresentada a capacidade cibernética associada às operações de informação, que é uma capacidade relacionada às operações de informação.

---

* Chefe do Centro de Defesa Cibernética.

O CDCiber foi criado em 2010 com a finalidade de implantar o setor cibernético no âmbito do Exército Brasileiro e da defesa do país. Contudo, ao longo dos anos o CDCiber começou a ser empregado também em operações, vindo a registrar em 2012 o seu primeiro emprego em grandes operações:

Figura 1 - A evolução do Centro de Defesa Cibernética

Fonte: o autor, 2019.

Nessa época, o CDCiber contava apenas com 24 pessoas (desde o General ao Soldado mais moderno) e quando o CDCiber se deslocou para o Rio de Janeiro-RJ para atuar na Rio + 20, deparou-se com um Centro que havia sido montado especificamente para esse evento muito maior, cerca de 110 pessoas. Esse fato proporcionou um aprendizado gigantesco para a Defesa, na medida em que um estabelecimento que ainda era incipiente havia recebido a missão de coordenar a segurança e a defesa cibernética de um grande evento, gerenciando uma estrutura muito mais robusta do que estava acostumado (cerca de 110 componentes). Nessa ocasião, a participação de todos os órgãos envolvidos com a segurança cibernética do país, possibilitou ao CDCiber adquirir experiência, tanto no trabalho de forma articulada, como no trabalho em interagências.

Essa trajetória revela o aprendizado que o CDCiber adquiriu desde a sua criação. Após a Rio + 20, o CDCiber foi empregado nos grandes eventos esportivos, os quais requeriam uma complexidade muito maior no planejamento e na execução das missões. A necessidade de se desdobrar destacamentos em várias cidades do país durante a copa do mundo e a copa das confederações exigiu esforço adicional aos integrantes do CDCiber. Desde então, o Centro tem atuado de forma articulada em todo o território nacional e sempre sob a forma de interagências.

O Exercício Guardião Cibernético só foi possível por causa do aprendizado adquirido ao longo desses anos. O exercício reúne considerável quantidade de órgãos

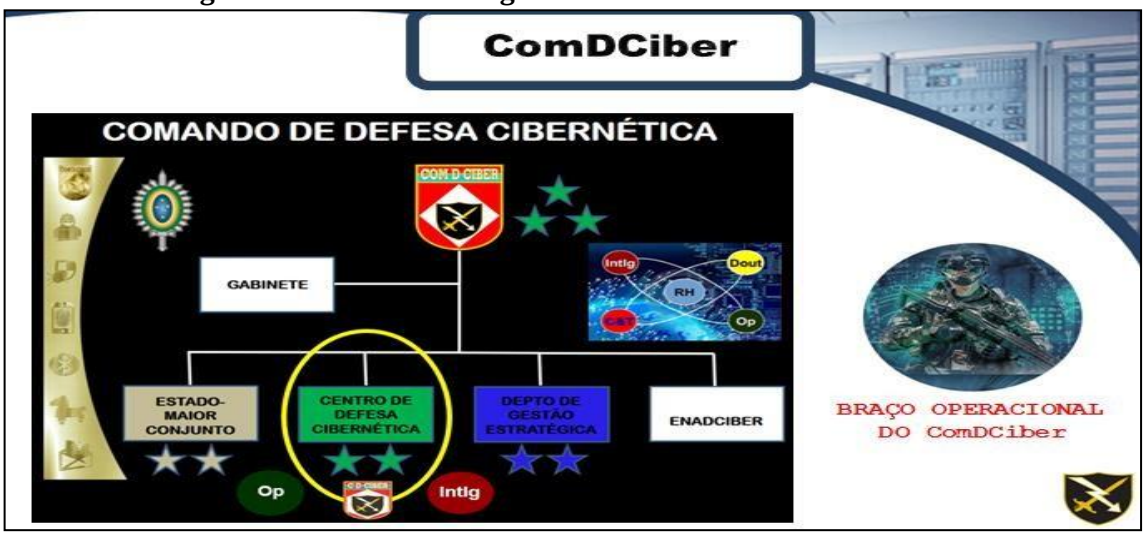
civis de diversas áreas estratégicas, os quais estão focados na resolução de problemas dentro de um contexto de cenário de crise no espaço cibernético nacional. Com essa experência acumulada, o CDCiber começou a compartilhar esse conhecimento com as nações amigas. Atualmente, há quatro militares brasileiros (um oficial e três sargentos) do CDCiber trabalhando juntamente com o Exército do Peru nos Jogos Pan-Americanos em Lima. Tendo em vista a realização dos Jogos Olímpicos de Tóquio em 2020, o CDCiber também está cooperando com os militares japoneses (já foram realizadas três reuniões de coordenação com os japoneses no sentido de compartilhar as experiências adquiridas nos Jogos Olímpicos do Rio de Janeiro). Esses aspectos são importantes, porque auxiliam no desenvolvimento do tema, bem como contribui no avanço do trabalho com países de nossa região e fora dela.

2. Desenvolvimento

A base do trabalho do CDCiber é a cooperação, pois essa atividade exige cooperação e atuação colaborativa. Sem isso, fica difícil a resolução de problemas. Dificilmente consegue-se descobrir o responsável pela ação cibernética. Ou seja, sem a colaboração, não vai chegar a lugar nenhum.

A figura abaixo apresenta a organização da Defesa Cibernética no país. Nela, o CDCiber é subordinada e considerada o braço operacional do Com DCiber:

Figura 2 - A estrutura organizacional da Defesa Cibernética



Fonte: o autor, 2019.

A nossa missão é executar ações cibernéticas, quais sejam: proteção, exploração e ataque cibernético no amplo espectro das operações, tanto em situação de paz, como em situações de crise e de conflito. Por seu turno, o manual de guerra cibernética define que essas três ações cibernéticas (proteção, exploração e ataque cibernético) precisam

transformar-se em capacidades. Dessa forma, a capacidade militar terrestre cibernética está composta por três capacidades operativas: a proteção cibernética, a exploração cibernética e o ataque cibernético.

Para o Exército Brasileiro, o CDCiber é uma força de emprego estratégica. Ou seja, uma força de emprego estratégico empregado por módulos. O CDCiber nunca será empregado como um todo como as brigadas. O Centro pode ser empregado por meio de módulos especializados. Para cada missão, os módulos são organizados de acordo com a capacidade requerida, que irá variar de acordo com a necessidade e com a missão. Tendo cumprido estas etapas, a capacidade é entregue ao Comandante Operacional.

Figura 3 - Atuação do CDCiber por módulos especializados

Fonte: o autor, 2019.

No que concerne ao modo de trabalho, o CDCiber pode atuar de duas formas. Uma é com base no Centro de Operações Cibernéticas, que trabalha diariamente sob o contexto do Sistema Militar de Defesa Cibernética, incluindo o Exército Brasileiro, a Marinha do Brasil, a Força Aérea Brasileira, a Defesa em si e também as infraestruturas críticas de interesse da Defesa Nacional. O âmbito de atuação do CDCiber é bem amplo e o Centro de Operações Cibernética está em contato permanente com todos os órgãos que tratam da segurança cibernética no país trocando informações diariamente. Em linhas gerais, esse é o trabalho sistemático desempenhado pelo CDCiber, que é voltado para a proteção civil.

A segunda forma que o CDCiber pode atuar é como Força de Emprego Estratégico, sob a forma de módulos especializados. Esses módulos podem ser empregados tanto em operações militares, como também em apoio aos órgãos do sistema militar de defesa cibernética. Ou seja, se há um sistema crítico ou se uma força específica

da Força Aérea Brasileira (FAB) está solicitando apoio ao CDCiber, esse apoio se dá com base nos módulos especializados.

Figura 4 - Situações de emprego do CDCiber

Fonte: o autor, 2019.

A organização do CDCiber é muito enxuta e simples. É composto por uma Subchefia, um Estado-Maior pessoal, uma Divisão de Proteção, uma Divisão de Exploração e uma Divisão de Apoio Operacional. Partes das capacidades do CDCiber são organizadas em áreas funcionais.

Figura 5 - Estrutura organizacional do CDCiber

Fonte: o autor, 2019.

Coerente com a concepção estratégica do EB como Força de Emprego Estratégica, o primeiro princípio de atuação do CDCiber é a atuação colaborativa. Tal princípio se justifica pela necessidade que se tem em ampliar as relações com todos os órgãos envolvidos no assunto, tanto em nosso país, como em países amigos.

O segundo princípio de atuação do CDCiber é a modularidade. O Centro sempre será empregado por módulos especializados.

O terceiro princípio de atuação é a flexibilidade, pois exige que esses módulos sejam flexíveis e organizados de acordo com a capacidade requerida para determinada missão. Ou seja, dependendo da missão, a configuração desse módulo vai variar.

O quarto princípio de atuação do CDCiber é adaptabilidade. Os componentes do CDCiber (Oficiais, Subtenentes e Sargentos) poderão estar trabalhando num sistema de informação da Força Aérea Brasileira (num sistema de controle do espaço aéreo), ou também podem estar trabalhando num sistema de informação da Marinha do Brasil (num sistema de controle naval), ou também podem estar trabalhando numa rede corporativa de um órgão da administração pública federal. Ou seja, o conhecimento desse especialista se aplica em várias situações, pelo que gera considerável complexidade para a capacitação desse especialista. Esse profissional precisa estar em condições de se adaptar ao cenário que se encontra.

O quinto princípio de atuação do CDCiber é a elasticidade, que por sua vez, está correlacionado com o último princípio de atuação do CDCiber, que é a sustentabilidade. O tipo de apoio prestado pelo CDCiber normalmente se alonga no tempo e, por isso, requer esforço adicional no sentido de manter esse apoio, evidenciando as características de elasticidade e sustentabilidade. O CDCiber registra casos de apoio a determinados órgãos em Brasília-DF que duraram mais de um ano com a equipe do Centro prestando esse tipo de apoio.

No tocante às áreas funcionais, constata-se a presença de seis. A primeira delas é a análise de incidentes. Hoje, existe uma solução integradora no Centro de Operações Cibernéticas, que recebe os dados provenientes de órgãos parceiros ou de órgãos pertencentes ao sistema. Sob o conceito de *big data*, incorpora inteligência artificial nesses dados para poder gerar alertas automatizados para os órgãos do sistema.

É interessante essa massa de dados que eu tenho para poder fazer a inteligência da ameaça cibernética. É uma proposta que só o Com DCiber está fazendo porque somente ele tem como receber uma massa de dados grande, oriunda de todas as forças de órgãos parceiros e transformá-las em conclusões factíveis. Por exemplo, se um IP do exterior está realizando uma atividade maliciosa na infraestrutura da Força Aérea Brasileira na tentativa de identificar vulnerabilidades, isso é compartilhado de imediato com o Centro de Operações Cibernéticas. Será que esse IP está fazendo a mesma coisa nas outras estruturas ligadas à defesa? Será que esse IP é novo ou começou esse incidente de novo? Será que esse IP já nos visitou anteriormente em outras forças na defesa? Feito essas perguntas, a análise passa a ser automatizada e inserida na base de dados. O CDCiber

verifica a diversidade de organizações que compartilham notificações conosco e aquelas que também recebem nossas notificações. Essa é a base da articulação do compartilhamento da informação com as organizações para que elas possam se proteger.

Um caso recente e bem interessante envolveu um IP, que fez uma ação em força sobre um determinado órgão e depois acabou sendo identificado. Esse IP fez a mesma tentativa de ação em força em outros órgãos e quando nós informamos aos órgãos, os mesmos bloquearam esse IP. Ou seja, é um trabalho de prevenção, porque o importante é poder prevenir essas ameaças. Esse é o trabalho principal do CDCiber. Estar à frente daquela ameaça, compartilhando essa informação com todos os demais de sua equipe de segurança.

A segunda área funcional é a pesquisa e análise e inteligência de ameaças. Essa área aprofunda o estudo sobre as ameaças cibernéticas e sobre os agentes de ameaça. Com base nessa área funcional, o CDCiber acompanha os grupos que fazem ação sobre os órgãos de governo, sobre os órgãos das forças com frequência. Isso tudo a gente percebe porque se repete.

A análise sobre esses grupos procura responder os seguintes questionamentos: Como é a rede de relacionamento desses grupos? Qual a intenção dessas organizações em expor dados sensíveis? A intenção é meramente de promoção pessoal ou de um determinado grupo *hacker*? Quais são as técnicas, táticas e procedimentos desses atores? Como os mesmos atuam? Tem algo novo ou alguma ação nova? Como eles chegaram nessa essa informação? Como é a rede de relacionamento desses grupos? Qual a intenção dessas organizações em expor dados sensíveis? A intenção é meramente de promoção pessoal ou de um determinado grupo *hacker*?

Quem faz esse trabalho diariamente precisa utilizar ferramentas para agilizar o trabalho, da mesma forma para torná-lo mais qualitativo. Por exemplo, existe uma plataforma de compartilhamento de ameaças cibernéticas, que começou com o compartilhamento de uma determinada ameaça e depois se ampliou para ameaças cibernéticas em geral. Cerca de seis mil organizações utilizam essa solução e compartilham informação sobre as ameaças. Neste espaço se compartilham as características e os indicadores de comprometimento que caracterizam a presença daquela ameaça.

Se a ameaça aparece no tráfego de determinada instituição, a mesma bloqueia. Para isso, é necessária uma massa de especialistas atuando em prol da atividade. Na verdade, poucas organizações contam com isso. Pode-se dizer que é um serviço agregado

que o CDCiber entrega para as organizações, porque as mesmas não têm capacidade de fazer isso no dia a dia.

A terceira área funcional é a análise de riscos. Isso faz parte da segurança operacional, pelo que se deve ter isso sempre em mente. Diante do exposto, torna-se necessário provocar uma mudança em nossa cultura de planejamento e em nossa cultura organizacional. Não dá para trafegar nesse ambiente, querer ter imagem, querer ter sistemas de apoio à decisão, redes, se não pensar em segurança. Ou seja, é imperioso que haja uma revolução nos nossos planejadores, no nosso dia a dia. Não dá pra montar um Centro de Operações *ad hoc* para conduzir uma determinada operação querendo usar tecnologia e não pensar em segurança. Essa área funcional atua em torno das questões de segurança que envolve o ambiente cibernético.

A quarta área funcional é a defesa ativa. Um exemplo de defesa ativa que está sendo utilizada atualmente pelo CDCiber é o que o pessoal chama de teste de penetração ou teste de segurança. Realizam-se perguntas do tipo: Quais são os ativos existentes? Que tipo de *software* está sendo empregado? Esses *softwares* são vulneráveis? A configuração desses ativos está correta? Enfim, nossa doutrina precisa ter uma capacidade de ir aos nossos sistemas, propor correções para que os mesmos não sejam explorados por terceiros.

A quinta área funcional do CDCiber é análise de *malware*, que é complementar ao trabalho de análise de riscos. Depois da análise de riscos, é necessário verificar o que determinado vírus queria fazer naquele computador. Essa capacidade procura fazer exatamente isso, ou seja, analisar o motivo pelo qual o *malware* queria estar ali dentro. Se ele foi desenhado para estar naquela infraestrutura ou se algum usuário trouxe no seu *pendrive*, ou se estava presente na rede. Ou seja, esse tipo de análise é feito nessa área funcional.

A sexta área funcional, que é típica da atividade militar, é a identificação e exploração de vulnerabilidades ou ataque cibernético, em outras palavras. É necessário verificar quais capacidades as Forças Armadas possuem e que estão voltadas para a exploração dos sistemas alvo dentro de uma operação militar.

A figura a seguir apresenta as áreas funcionais existentes no CDCiber. Essas áreas funcionais determinam as equipes de trabalho, os postos de trabalho, à forma como o CDCiber será empregado, a área de especialização necessária para os militares do Exército Brasileiro, da Marinha do Brasil e da Força Aérea Brasileira, dentre outras

questões. A organização do módulo especializado vai depender do que há disponível e do tipo de apoio que precisa ser prestado.

Figura 6 - Áreas funcionais

Fonte: o autor, 2019.

As hipóteses de atuação são muito importantes porque orientam o emprego do CDCiber. Foi feito um exercício internamente com integrantes do Estado-Maior do CDCiber e com vários especialistas para ver os cenários o CDCiber poderia ser empregado. Tal exercício foi concebido com a finalidade do Centro estar apto para fazer frente a essas hipóteses. O trabalho do CDCiber foi empregar as equipes, os módulos em apoio as estruturas estratégicas do país, quais sejam: Polícia Federal, GSI, gabinete da presidência, etc. Apoiar em pessoal e material os sistemas de informação críticos de interesse da Defesa.

Dessa forma, evidenciou-se a importância do CDCiber ter equipes prontas para cumprirem suas missões, pelo que se evidenciou o conceito de concepção estratégica "prontidão operativa" nas atividades do Centro. Basta receber uma ligação telefônica, que a equipe sairá para prestar o apoio à organização ou ao sistema crítico no apoio à recuperação de sistemas que tenham sido infectados ou comprometidos.

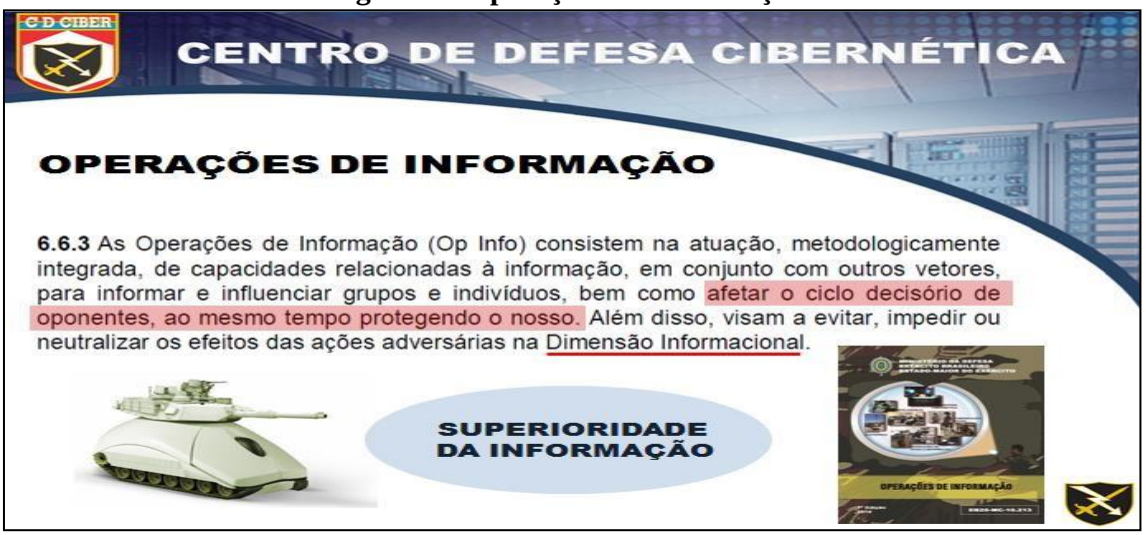
O CDCiber emprega suas capacidades para agregar poder de combate nas missões militares. No contexto de uma operação militar, o CDCiber pode ser empregado sob a forma de uma Força Conjunta de Guerra Cibernética ou por meio de Destacamentos Conjuntos de Guerra Cibernética. A Força Conjunta de Guerra Cibernética contará com componentes do CDCiber, do Exército Brasileiro, da Marinha do Brasil e da Força Aérea Brasileira.

Não há dúvida de que se houver mais um grande evento no Brasil, a Defesa será novamente convidada a coordenar e quem vai fazer isso será o ComDCiber. Essa área

está em constante desenvolvimento, pelo que não confere ao CDCiber a garantia de que o mesmo está bem. Muito pelo contrário, isso é uma caminhada que não tem fim, porque essa tecnologia muda todos os dias. A ameaça se transforma todos os dias. O acompanhamento precisa ser integral. Se aparecerem outras necessidades, outras capacidades serão incorporadas ao CDCiber.

No tocante às operações de informação, nota-se que o objetivo síntese de sua missão é a obtenção da superioridade de informação junto às demais capacidades anteriormente comentadas. No que diz respeito à atuação, verifica-se nos planejamentos de operação de informação, que a grande preocupação está em atuar na informação do oponente. Todavia, a proteção da nossa informação crítica é fundamental. Ou seja, o CDCiber atua também na proteção das nossas informações operacionais críticas.

Figura 7 - Operações de Informação



Fonte: o autor, 2019.

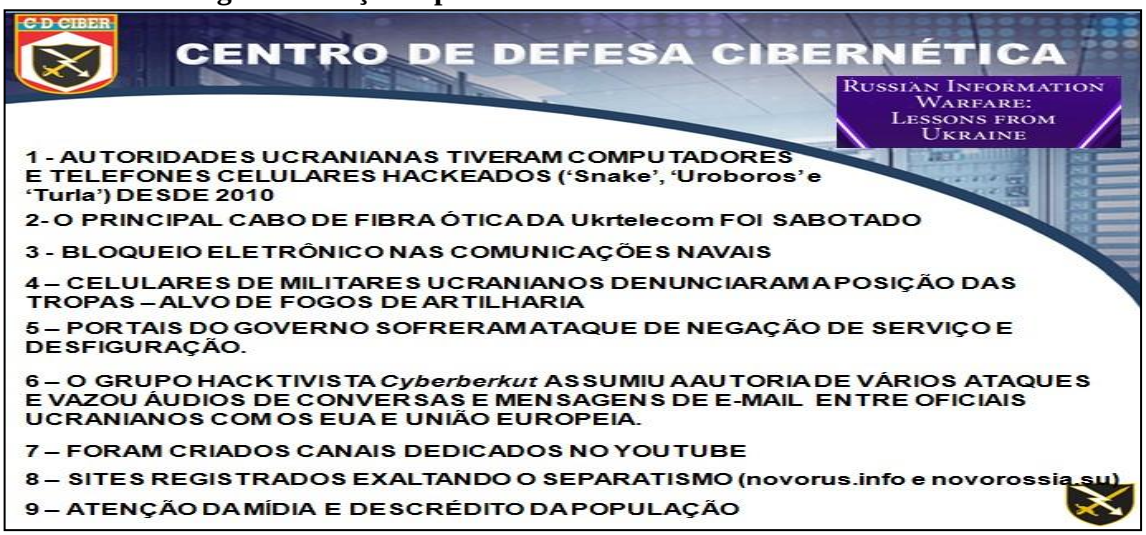
O ambiente que conduz as operações de informação precisa ser protegido para evitar que o mesmo se torne alvo de um ataque cibernético e por consequência tenham o local, a equipe e a máquina identificados pelo oponente. Há que se ter uma grande preocupação com a segurança operacional e com a própria segurança dos produtos digitais.

Se um produto for lançado na *internet* sem o devido cuidado, vai deixar rastros e os mesmos carregarão consigo uma série de informações associadas. Da mesma forma, entende-se que deve ter cuidado também com o celular, particularmente na segurança do ambiente operacional do celular. Nos dias atuais, o celular representa o que tem de mais frágil no mundo, pois podem ser extraídas informações do tipo: nosso ambiente operacional, localização de tropas e autoridades, celulares infectados, dentre outras questões. Em síntese, a segurança pessoal é determinante para o sucesso nas operações

militares, uma vez que o nosso pessoal pode ser alvo de ataques cibernéticos e, dessa forma, revelar detalhes importantes.

O exemplo mais emblemático desse tipo de atuação repousa no conflito entre a Ucrânia e a Rússia, onde houve várias ações fazendo uso das fragilidades do aparelho celular. A figura a seguir elenca as lições aprendidas relativas ao ambiente cibernético deste conflito:

Figura 8 - Lições aprendidas do conflito Rússia x Ucrânia



Fonte: o autor, 2019.

3. Conclusões

Como conclusão, pontua-se que o CDCiber pode atuar também no sentido de obter informações, identificar lideranças digitais, identificar perfis falsos, levantar e analisar de vínculos, realizar campanhas de informação e também atuar sobre a informação para manipular o que destruir, atuar sobre a infraestrutura, etc.

Interessante destacar que o CDCiber representa uma nova capacidade nas operações militares em todos os níveis. Agradeço a oportunidade que me foi dada e termino a apresentação do CDCiber e suas capacidades.

Muito obrigado pela atenção!

O COMANDO DE COMUNICAÇÕES E GUERRA ELETRÔNICA DO EXÉRCITO (CCOMGEX)

General de Brigada Carlos Alberto Dahmer*

1. Introdução

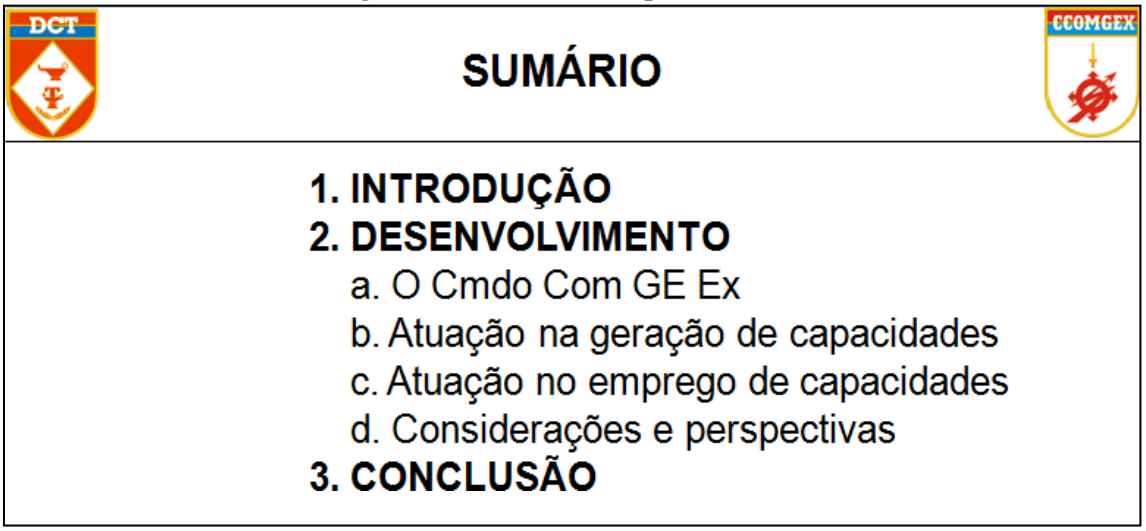
Boa tarde a todos.

É uma satisfação enorme estar nesta casa novamente depois de 15 anos. É um momento ímpar poder voltar a fazer uma apresentação sobre o Comando de Comunicações e Guerra Eletrônica do Exército (CCOMGEX). Sob o contexto da cibernética, o objetivo é apresentar a atuação do CCOMGEX na geração e no emprego de capacidades de defesa cibernética junto ao Exército Brasileiro (EB).

O CCOMGEX é um grande comando desconhecido do EB. No ano passado, numa conversa que tive com o General Villas Boas - então Comandante do Exército Brasileiro, explicava para ele sobre a geração de capacidades proporcionada pelo curso de guerra cibernética e pelo curso de proteção cibernética realizado no CCOMGEX e comentei também que provavelmente a maioria dos militares da instituição não deve conhecer o trabalho desenvolvido pelo CCOMGEX, que prontamente concordou com a minha opinião.

Diante do exposto, a apresentação de hoje focará no trabalho desenvolvido pelo CCOMGEX. Para isso, seguirá o roteiro apresentado a seguir:

Figura 1 - Sumário da apresentação



Fonte: o autor, 2019.

* Comandante de Comunicações e Guerra Eletrônica do Exército Brasileiro.

2. Desenvolvimento

O CCOMGEX foi criado em 1984. Essa data é emblemática, pois em 1982 houve o conflito das Malvinas, na Argentina. Nesse conflito, foi verificada a atuação de forças de guerra eletrônica do Exército Inglês, que se mostrou fundamental na vitória inglesa. Diante dessa realidade, o Exército Brasileiro sentiu a necessidade de ter uma força semelhante e em 1984 criou uma força de guerra eletrônica, que foi considerada o marco inicial da história de evolução de guerra eletrônica no Brasil.

Anos mais tarde, em 1991, o EB criou a primeira unidade operacional em guerra eletrônica (1ª Companhia de Guerra Eletrônica), localizada dentro das instalações do Forte Marechal Rondon.

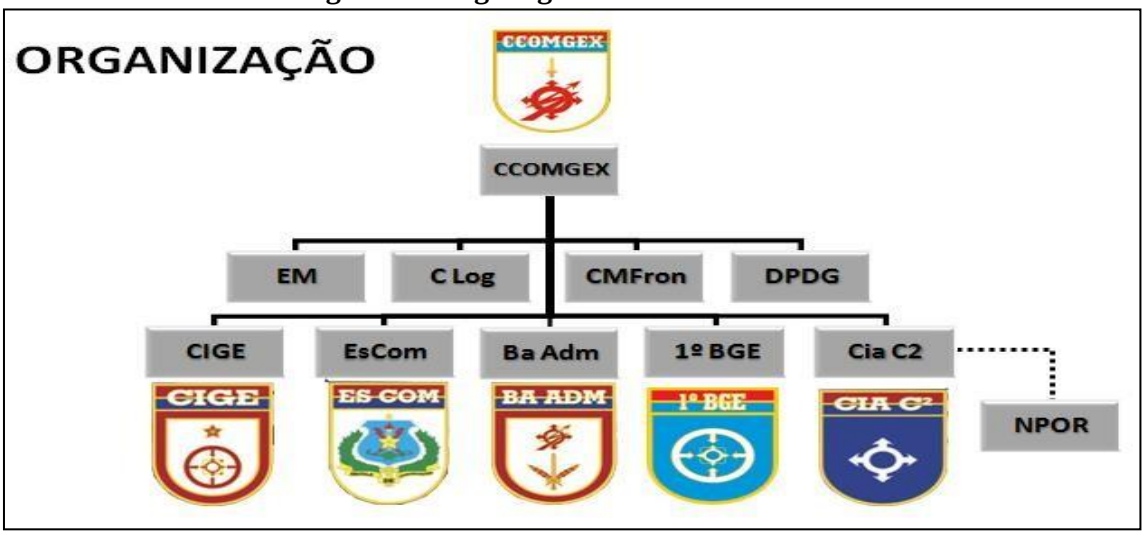
Dando continuidade a expansão da Guerra Eletrônica no seio da instituição, o Exército Brasileiro criou o Centro Integrado de Guerra Eletrônica (CIGE) em 1998. Quase dez anos depois, já em 2007, a então Diretoria de Material de Comunicações, Eletrônica e Informática (DMCEI) foi transferida para as instalações do CIGE. Em 2009, a sua estrutura foi radicalmente modificada com a união da antiga Diretoria de Material de Comunicações e Eletrônica com as estruturas do CIGE, vindo a se transformar no CCOMGEX. Nesse ano, também foram criadas a Base Administrativa e a Companhia de Comando e Controle, que é a Unidade de comunicações de comando e controle dentro do Forte Marechal Rondon.

Dois anos depois, em 2011, houve outro fato importante. Agregou-se mais uma Escola nesse complexo: a Escola de Comunicações (EsCom), que foi transferida do Rio de Janeiro-RJ para a cidade de Brasília-DF. Cumpre ressaltar que a EsCom é a escola mais antiga de especialização do EB, indo completar 100 anos de existência em 2021.

Em 2012, ficou decidido que o projeto estratégico SISFRON ficasse sob a égide do CCOMGEX e que o órgão iniciasse os esforços do EB nesse projeto estratégico. Em 2013, o Exército Brasileiro transformou a então 1ª Companhia de Guerra Eletrônica no 1º Batalhão de Guerra Eletrônica, fato que ressalta o aumento de importância desse tema na instituição.

No ano de 2016, o CCOMGEX passou a ser um Comando de Comunicações e Guerra Eletrônica, haja vista sua vertente operacional. No ano seguinte, em 2017, ocorreu a consolidação da atual estrutura com a chegada do setor cibernético nas instalações do Forte Marechal Rondon, conforme especificada a seguir:

Figura 2 - Organograma do CCOMGEX

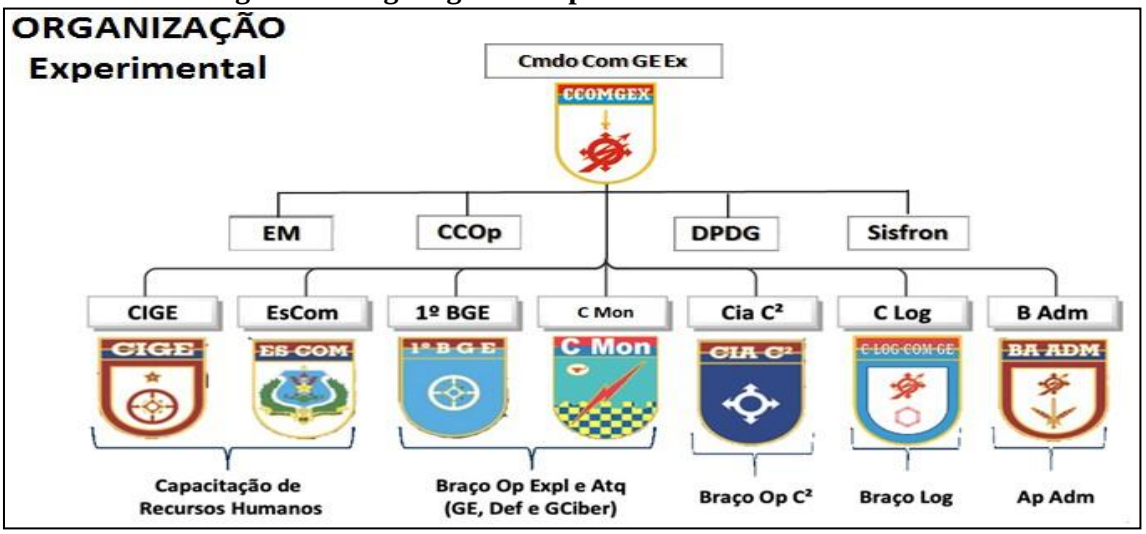


Fonte: o autor, 2019.

O CCOMGEX conta com uma organização militar típica: cinco unidades e a estrutura de um Estado-Maior. Há duas Escolas de capacitação de recursos humanos, uma Base Administrativa, um braço operacional (o Batalhão de Guerra Eletrônica, que atua em prol do SISFRON) e a Companhia de Comando e Controle, que tem sob sua responsabilidade o Núcleo de Preparação de Oficiais da Reserva (NPOR).

Com as mudanças ocorridas na sociedade e o consequente aumento de importância da cibernética nos últimos anos, o CCOMGEX sentiu a necessidade de mudar a sua estrutura, pelo que propôs uma organização em caráter experimental, sinalizada na sequência:

Figura 3 - Organograma experimental do CCOMGEX



Fonte: o autor, 2019.

Em síntese, estão sendo propostas a criação de mais Unidades Militares, uma voltada para a parte operacional e outra voltada para a parte logística. Outro fato que deve

ser destacado é a criação do Centro de Coordenação de Operações, que vai coordenar as operações no Brasil inteiro e vai entregar os meios necessários para os Comandos Militares de Área.

A atuação do CCOMGEX engloba atividades como a capacitação de recursos humanos, operações de logística com todos os seus encargos (compra de material, distribuição e manutenção), aspectos doutrinários (todos os manuais de comunicações e guerra eletrônica contribuem com a parte cibernética), operações militares e realização de parcerias com instituições de interesse.

O CCOMGEX é uma agência de inovação. O próprio SISFRON já gerou duas patentes de inovação tecnológica. Como foi dito anteriormente, o CCOMGEX participa de operações no Brasil inteiro, com grande incidência em missões de apoio em comando e controle, apoio à área de inteligência, guerra eletrônica e guerra cibernética. Além disso, o CCOMGEX é responsável pela implantação de um dos maiores programas estratégicos do país: o SISFRON.

Em termos operacionais, o CCOMGEX conta com duas Organizações Militares: o 1º Batalhão de Guerra Eletrônica (BGE) e a Companhia de Comando e Controle (Cia C^2). Essas Unidades trabalham por meio de módulos de emprego estratégico. São as duas únicas unidades da Força Terrestre de emprego estratégico.

Em termos de capacitação, o CCOMGEX conta com duas Escolas: o Centro de Instrução de Guerra Eletrônica (CIGE) e a Escola de Comunicações (Es Com). Um dos lemas, uma das frases emblemáticas do CIGE é "berço da guerra cibernética", porque em 2007 o CIGE começou a sentir necessidade de iniciar/desenvolver/ministrar cursos voltados para a guerra cibernética. Atualmente, o CIGE oferece vários cursos voltados para a guerra cibernética, destinados tanto para oficiais, como para profissionais de nações amigas, como para sargentos também. Nesse rol de cursos, destacam-se os seguintes: 1) o planejamento de guerra cibernética e eletrônica (destinado somente para oficiais do EB); e 2) o estágio internacional de defesa cibernética para ONA (destinado para profissionais de nações amigas).

No que concerne à Es Com, verifica-se que a mesma ministra cursos mais técnicos, voltados para o comando e controle, e comunicações. Dentre os cursos oferecidos pela Es Com, destacam-se dois: 1) Operador de TIC e; 2) o estágio de proteção cibernética. Importante pontuar que já tem uma proposta no Estado-Maior do Exército (EME) para transformar o estágio de proteção cibernética em curso de proteção cibernética, com uma duração aproximada de 12 semanas.

Outro aspecto interessante acerca da Es Com é a existência do portal de ensino à distância. Esse portal possui 87 cursos ligados às comunicações, comando e controle. São cursos gratuitos para militares em geral. Já é o terceiro ano seguido que o CCOMGEX ganha o prêmio de melhor academia da América do Sul. Esse ano há 3.500 inscritos. No ano passado, houve 12 mil inscritos.

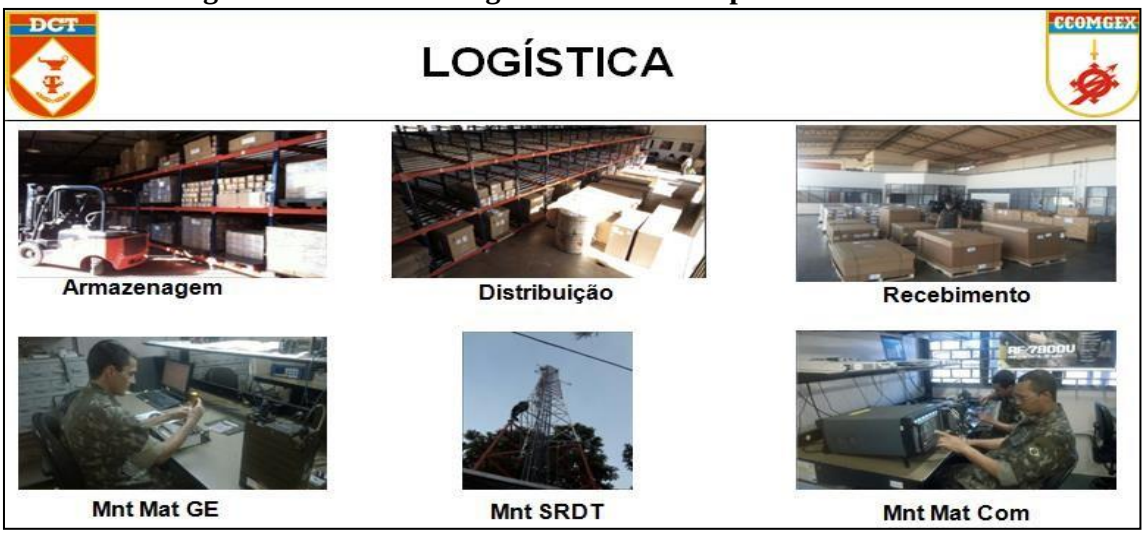
Figura 4 - Instituto Rondon de Capacitação Continuada (IRCC)

CAPACITAÇÕES DISPONIBILIZADAS PELA ESCOM	Capacitações gratuitas no mercado, centralizadas e classificadas por área:	
Cursos: • Harris (Instruções, manuais, softwares e firmwares dos rádios) • Sotas (Instruções, manuais, vídeo aulas e softwares) • C2 Cmb (Manuais de instalação, configuração e operação) • Motorola (Cursos básicos e guia do usuário sobre os rádios) • Eletrônica (Curso básico em eletrônica digital)	02	Área de Cibernética
	33	Programação de Software
	03	Redes de Computadores e Virtualização
Outros: • Grupo de Assessoramento Técnico de Comunicações, Guerra Eletrônica e Guerra Cibernética (GATComGECiber) • Comitê Gestor do Sistema de Comando e Controle do Exército (CGSC²Ex) • Gestão do Conhecimento DPDG • Grupo Permanente de Produção Doutrinária do Cmdo Com GE Ex • SAD SISFRON Fases 2 e 3ª	05	Diversos na área de TI
	01	Eletrônica, Eletricidade e Manutenção
	02	Edição de Imagens
	16	Administração Pública
	10	Cursos de Idiomas
	15	Diversos
Total: 05 cursos / 05 Grupos de Trabalho	Total de cursos: 87	

Fonte: o autor, 2019.

Há também a vertente logística desenvolvida no CCOMGEX (aquisição, armazenagem, suprimento, manutenção e transporte de todo o material de comunicações e guerra eletrônica de campanha). Essas são algumas das imagens do trabalho desencadeado pelo CCOMGEX no dia a dia:

Figura 5 - Atividades logísticas realizadas pelo CCOMGEX



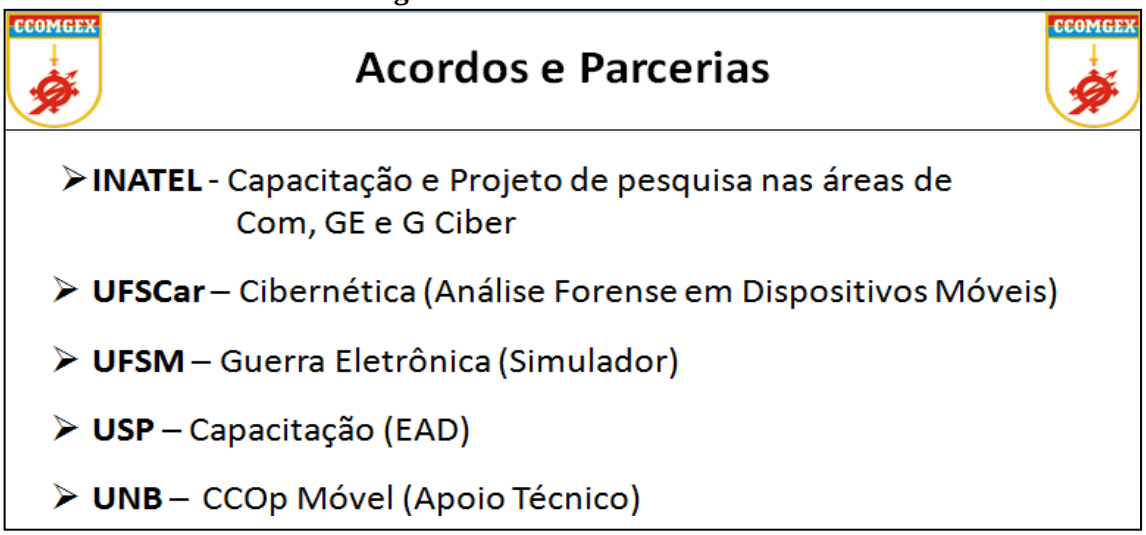
Fonte: o autor, 2019.

Há também a Divisão de Planejamento, Doutrina e Gestão (DPDG), que é uma divisão que faz planejamentos de gestão estratégica e que coopera com a doutrina de comunicações, guerra eletrônica e cibernética através de manuais de prospecção

tecnológica e provas de conceito. Além disso, estabelece relações institucionais com foco na doutrina, assessoramento técnico na parte da ciência, tecnologia e inovação.

O CCOMGEX estabelece também parcerias estratégicas, gestão de acordos de *offset* e cooperação no desenvolvimento de sistemas e materiais de emprego militar:

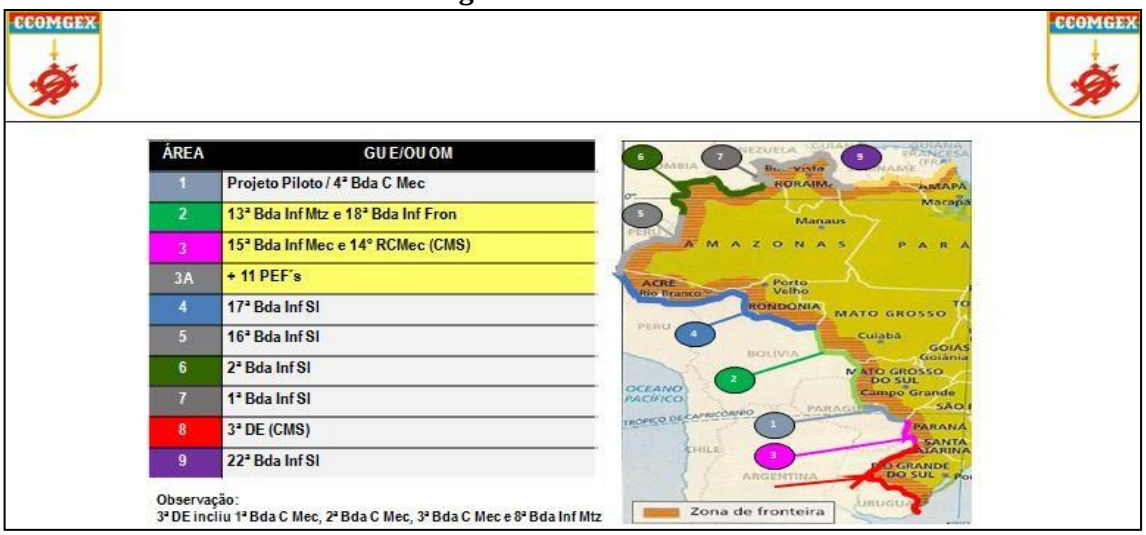
Figura 6 - Acordos e Parcerias



Fonte: o autor, 2019.

Nesse rol de parceiros, o destaque é fica por conta da parceria feita com a Universidade Federal de São Carlos, na área de cibernética. É um instrumento que o CCOMGEX trabalha e busca aproveitar as *expertises* da academia para também capacitar os nossos instrutores.

Figura 7 - SISFRON



Fonte: o autor, 2019.

A concepção de monitoramento do SISFRON está baseada em três vertentes, a saber: sensoriamento, apoio à decisão e apoio à operação. Dessa forma, o CCOMGEX é responsável por todo sensoriamento e apoio à decisão. Atualmente, o CCOMGEX está

participando da implantação do projeto piloto do SISFRON no Estado de Mato Grosso do Sul.

Cumpre destacar que o projeto de implantação do SISFRON na fronteira brasileira está concebido em três fases. A primeira está quase se encerrando. A segunda fase está em curso e prestes a terminar e a terceira fase prevê a entrega de material para os pelotões de fronteira, que é uma necessidade regional do Comando Militar da Amazônia. A figura seguinte sintetiza essas fases:

Figura 8 - Fases de implantação do SISFRON

Fonte: o autor, 2019.

O monitoramento da faixa de fronteira será realizado com ferramentas de sensoriamento e de apoio à decisão. Vários tipos de equipamentos serão utilizados nesse esforço, como por exemplo: radares transportáveis, radares móveis, binóculos termais e binóculos multifuncionais. Ou seja, um conjunto de guerra eletrônica. Para isso, foi construída uma infovia para o transporte dessas informações: centro de comunicações móveis, *softwares* e etc.

O foco da atuação do CCOMGEX está centrado na geração de capacidades, no nível tático. O CCOMGEX trabalha para a Força Componente, ou seja, gerando capacidades para o EB e para a Força Terrestre. Embora os cursos sejam ofertados para os militares das demais Forças Armadas e para integrantes da sociedade, a maior parte das vagas é destinada para o Exército Brasileiro.

Figura 9 - Nível de atuação do CCOMGEX em Guerra Cibernética

Fonte: o autor, 2019.

Em termos de capacidades, entende-se que o CCOMGEX vai gerar capacidade militar terrestre de cibernética, que por sua vez envolve as seguintes capacidades operativas: proteção cibernética, exploração cibernética e o ataque cibernético. Essas capacidades precisam ser desenvolvidas para que as mesmas sejam empregadas na Força Terrestre. Para gerar essas três capacidades, o CCOMGEX conta com o Centro de Coordenação de Operações, o CIGE, os elementos de operação e a Companhia de Guerra Cibernética do 1º BGE.

O adestramento nessa área, pelo menos para a força terrestre, tem sido feito sempre conduzido pelo 1º BGE. Para fins operacionais, verifica-se que a Companhia de Guerra Cibernética, oriunda do 1º BGE, tem capacidade de realizar todas as três ações: proteção, exploração e ataque. As seções de cibernética do Batalhão de Comunicações, por seu turno, tem a capacidade de fazer somente a exploração e a proteção. E as seções de proteção cibernética só estão aptas a realizar a proteção.

Destaco a tendência mundial nos dias atuais em juntar a guerra eletrônica com a guerra cibernética no nível tático. Entretanto, essa tendência não é verificada no nível estratégico e no nível operacional. Nesses níveis, a guerra eletrônica tem uma estratégia diferente da guerra cibernética.

Nas questões afetas ao adestramento, nota-se que o mesmo é dividido em duas vertentes: 1) Capacitação Técnica e Tática do Efetivo Profissional (composto por três fases: a primeira é levantar a ferramenta de ataque exploração; a segunda é a proteção cibernética; e a terceira é o desenvolvimento de soluções); e 2) Adestramento Básico e Avançado (Programa de Adestramento Básico e Programa de Adestramento Avançado).

De todas as atividades de adestramento realizadas pelo CCOMGEX, toma destaque a Manobra Escolar, que hoje é um dos maiores exercícios que o CCOMGEX participa em termos de manobra. Todo ano, o CCOMGEX emprega o 1º BGE neste exercício aplicando as ferramentas cibernéticas.

Figura 10 - Adestramento realizado pelo 1º BGE em 2019

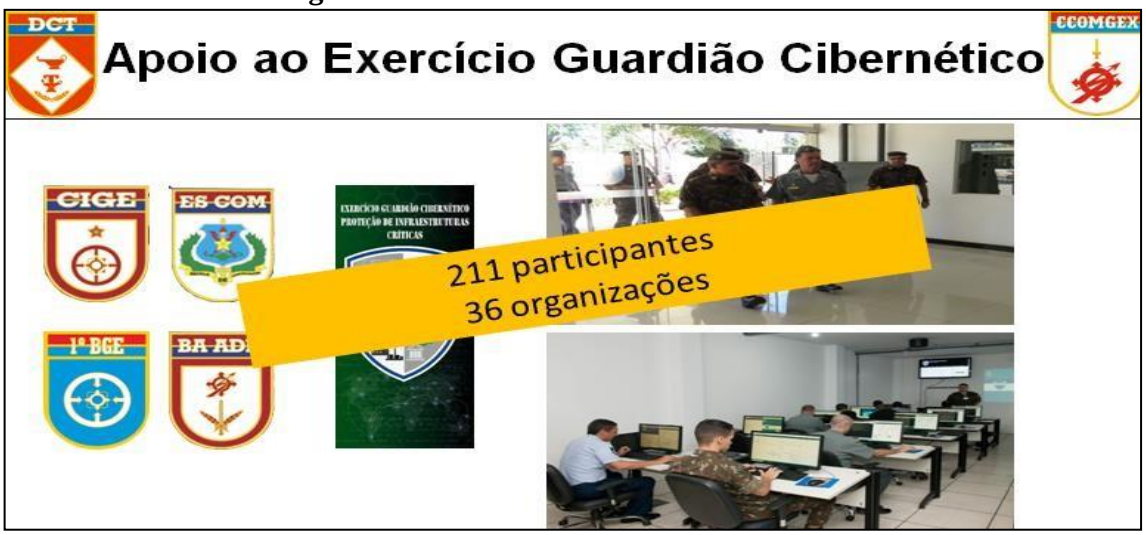
Fonte: o autor, 2019.

Um ataque cibernético é desencadeado da seguinte forma: reconhecimento, escaneamento e exploração da vulnerabilidade, manutenção do acesso e cobertura de rastros. A primeira tarefa é o reconhecimento, momento que será utilizada as fontes abertas, as redes rádios que estejam funcionando e o mapeamento das redes. A segunda tarefa é o escaneamento, ocasião em que será buscada a vulnerabilidade e verificar como pode adentrar no sistema. A terceira tarefa é a exploração da vulnerabilidade, ou seja, o ataque cibernético propriamente dito. Materializa-se no acesso para adquirir dados para corromper algo. A quarta tarefa se consiste nas atividades realizadas com o propósito de manter o acesso. E a quinta fase é denominada de cobertura dos rastros, que é fundamental numa campanha de operação de informações. Se não for bem feita, compromete toda a campanha.

Conforme descrito anteriormente, com relação à educação, o CCOMGEX conta com duas escolas: CIGE e Es Com. O foco do CIGE está voltado para cursos e estágios de guerra cibernética profissionais (destaque para o Curso de Guerra Cibernética para Oficiais e Sargentos e para o Curso de Planejamento de Operações de Guerra Eletrônica e Guerra Cibernética para Oficiais). Por sua vez, o foco da Es Com está voltado para cursos mais técnicos, onde o idioma inglês está sendo bastante empregado (destaque para o Estágio de Proteção Cibernética).

O Exercício Guardião Cibernético é conduzido pelo Com DCiber e é extremamente importante para conscientizar as nossas estruturas críticas e estruturas estratégicas. Tal exercício contou com a participação de instituições civis e militares, perfazendo um total de 211 participantes e de 36 organizações:

Figura 11 - Exercício Guardião Cibernético



Fonte: o autor, 2019.

A guerra eletrônica e a guerra cibernética atuam fortemente no nível tático (sistemas que atuam simultaneamente no ambiente eletromagnético e no ambiente cibernético), diferentemente de níveis superiores. O 1º BGE possui grande capacidade de emprego no nível tático, pois fornece capacidade de guerra eletrônica e de guerra cibernética para a Força no nível tático. Para isso, o 1º BGE conta com duas Companhias de Guerra Eletrônica e uma Companhia de Cibernética.

Figura 12 - Integração da Guerra Eletrônica e da Guerra Cibernética no nível tático

Fonte: o autor, 2019.

Um exemplo da utilização das duas capacidades: na rede de uma força oponente há rádios táticos, redes de dados, voz segura GSM, celulares e outros equipamentos. Em

vista disso, a guerra eletrônica pode fazer bloqueio, interceptação, localizar e realizar um bloqueio no rádio e obrigar a força oponente usar outro tipo de material de comunicações. Assim, a cibernética pode atuar realizando a interceptação do celular, localizando o mesmo e realizando um ataque na posição onde se encontra o IP.

Durante a intervenção federal, o 1º BGE foi empregado ininterruptamente por um período de mais de um ano. A guerra eletrônica atuou realizando acompanhamento da localização do espectro magnético, levantando a força oponente nas áreas de atuação levantando as capacidades relacionadas à informação, apoiando a campanha com suas *expertises* cibernéticas, mapeando o ambiente, etc...

No conflito que envolveu a Rússia e a Ucrânia, observa-se que as forças russas empregaram a guerra cibernética. Nesse conflito, as forças russas utilizaram o conceito de guerra híbrida, atuando em todos os setores e disseminando a dúvida. Até hoje, a narrativa russa é a de que não empregou forças institucionais neste conflito e que o ataque cibernético foi feito por *hackers* patrióticos.

Figura 13 - Emprego de Guerra Cibernética no conflito Rússia X Ucrânia

Fonte: o autor, 2019.

Uma lição aprendida no conflito entre a Ucrânia e a Rússia foi o emprego macicço de foguetes de saturação de área para neutralizar as posições de artilharia ucranianas. Nessa ocasião, a capacidade de guerra eletrônica foi empregada no bloqueio do rádio, obrigando o soldado a utilizar o seu celular para tentar se comunicar, pelo que facilitou a localização do celular. Assim, foi feito um ataque cibernético contra as Brigadas da Ucrânia dentro do sistema de C², obrigando as tropas ucranianas a utilizarem o celular, o que facilitou o ataque russo. Dessa forma, os russos acabaram realizando o ataque onde a guerra eletrônica havia detectado o celular.

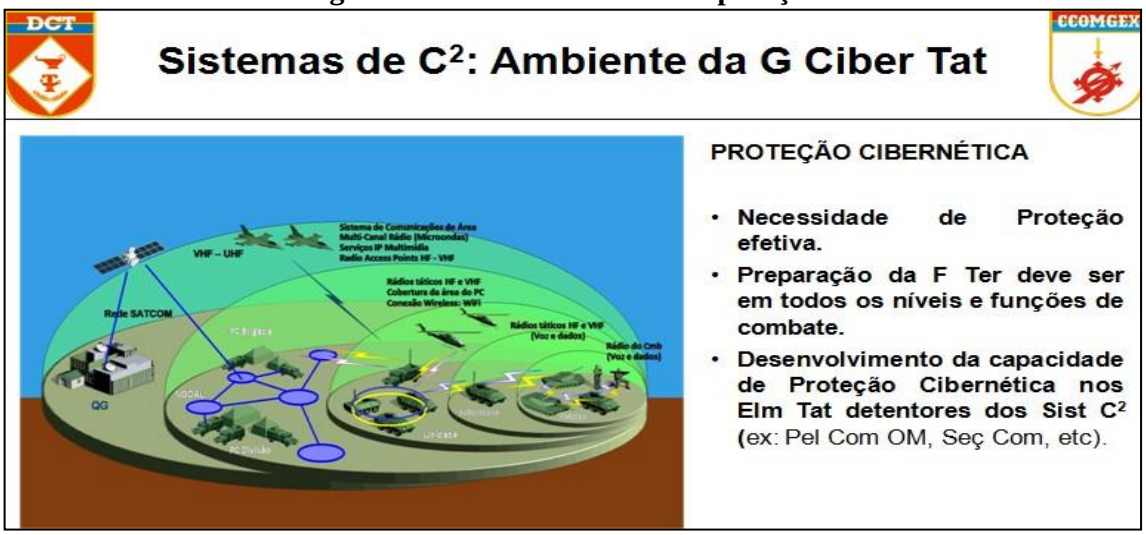
Figura 14 - Lições aprendidas no conflito Rússia X Ucrânia

Fonte: o autor, 2019.

As operações de informação existem desde a 1ª Guerra Mundial e durante a 2ª Guerra Mundial, elas foram muito empregadas nas operações de propaganda. Nos dias atuais, o maior emprego da cibernética tem sido legitimar às operações em curso. Como a cibernética tem acesso ao dispositivo móvel, ela tem sido usada como ferramenta nas operações de informação, ora falsificando, ora confirmando informações.

Essa seria a concepção de um sistema de comunicações típico em operações, abarcando desde o nível Pelotão até o nível Quartel-General, ou seja, desde o nível estratégico até o tático:

Figura 15 - Sistemas de C² em operações



Fonte: o autor, 2019.

Em missões dessa natureza, todos os rádios que são entregues para a Força Terrestre possuem IP. E se tem o IP, ele está trabalhando em rede, e se ele está numa rede cibernética, pode sofrer ataque cibernético. Encontrou a vulnerabilidade, o ataque será realizado e fatalmente será bem sucedido. O soldado no pelotão, lá na frente do campo

de batalha, não possui essa consciência. Se o Comandante do Esquadrão achar que não há problema usar o rádio IP na frente do campo de batalha, pode comprometer a missão, na medida em que o mesmo pode ser a porta de vulnerabilidade para toda a rede aqui, uma vez que tem IP.

Todos os senhores vão sair daqui para comandar Organizações Militares em um futuro bem próximo. Suas Unidades precisam ter essa consciência. Todas elas serão compostas de Seções de Proteção Cibernética. E as mesmas possuirão condições para isso. Ou seja, há uma necessidade de proteção efetiva em todos os níveis em funções de combate. Como foi falado anteriormente, às vezes o soldado acha que está tranqüilo fazendo a missão dele, mas ele pode ser a porta de entrada para uma vulnerabilidade que vai afetar toda a rede estratégica da operação.

O Comando de Defesa Cibernética sabe a responsabilidade que o CCOMGEX possui com os cursos de proteção, mas é insuficiente formarmos cerca de 20 a 25 alunos por ano. Por sorte, a academia agora também já está formando. Nos dias atuais, já há uma cadeira de cibernética na grade comum das universidades, mesmo que com uma carga horária incipiente.

O ataque de exploração até pode ter o *glamour* de fazer um ataque por gerar efeitos imediatos, mas a proteção cibernética consiste na principal missão da cibernética e para isso, o Centro de Defesa Cibernética atua 24 por 7 na proteção cibernética. Diante do exposto, ressalta-se que a proteção é muito mais importante do que a capacidade de ataque e exploração.

3. Conclusões

Como conclusão, entende-se que possuir a capacidade é dever da Força Terrestre e essa missão está sendo cumprida, pois estamos realizando exercícios de adestramento, estamos adquirindo materiais, dentre diversas outras ações em curso.

No que compete ao emprego, observa-se que a decisão foi tomada no mais alto nível. Ou seja, quando o CCOMGEX recebe uma ordem de empregar essa capacidade, alguém superior deu essa ordem, escudado numa legislação que permite fazer isso. O General Amim disse que a tomada de decisão é realizada no mais alto nível, pelo fato da guerra cibernética não respeitar as fronteiras. Por isso, o CCOMGEX toma muito cuidado nas atividades de adestramento e nas atividades reais.

Há que se ter muito cuidado no que está fazendo com o uso da cibernética em operações de informações, pois ela permite obter uma narrativa dominante. Eu fui a um

país e lá é diferente. Nesse país, a narrativa é assumida abertamente. Se há uma propaganda contra, o governo vai inundar a rede com outra narrativa para assumir o discurso. É uma maneira diferente de abordar, mas é uma forma. O Brasil não adota essa postura.

Usei a oportunidade para apresentar o CCOMGEX e mostrar como é a geração de capacidades realizada nesse comando.

Muito obrigado pela atenção!

OPERAÇÕES DE INTELIGÊNCIA E DE INFORMAÇÕES NO CONTEXTO DA GUERRA CIBERNÉTICA

Coronel Miler Barbosa das Neves*

1. Introdução

Bom dia a todos.

Eu gostaria de agradecer o convite para participar do XXI Ciclo de Estudos Estratégicos. Aproveito a oportunidade para cumprimentar o Professor Doutor Ricardo, todos os oficiais de nações amigas aqui presentes, aos representantes da Força Aérea Brasileira, da Marinha do Brasil e a todos os civis e alunos que nos prestigiam. Em 2007 e 2008 também estava na condição de aluno. Estava aqui sentado, fazendo algumas provas, de três, quatro horas de duração. E por isso, é muito bom regressar a essa casa e agradeço ao Comando da ECEME por essa oportunidade.

Figura 1 - Centro de Inteligência do Exército

Fonte: o autor, 2019.

Essa foto aérea é do Centro de Inteligência do Exército (CIE). Alguns companheiros de farda talvez nem tenham tido a oportunidade de colocar os pés dentro do CIE. A escola funciona no subsolo desse pavilhão. O CIE está com uma obra (outro pavilhão está sendo erguido), com previsão de término no próximo ano, ou, na melhor das hipóteses no final de 2019. Com isso, o CIE vai melhorar e muito a sua capacidade de especialização. Inclusive o novo comandante está aqui (Coronel Andrade, que é meu amigo particular) e deverá assumir o comando em fevereiro do ano de 2020. Poder estar nessa função e poder trabalhar como um vetor da atividade de inteligência das Forças

* Comandante do Centro de Inteligência do Exército.

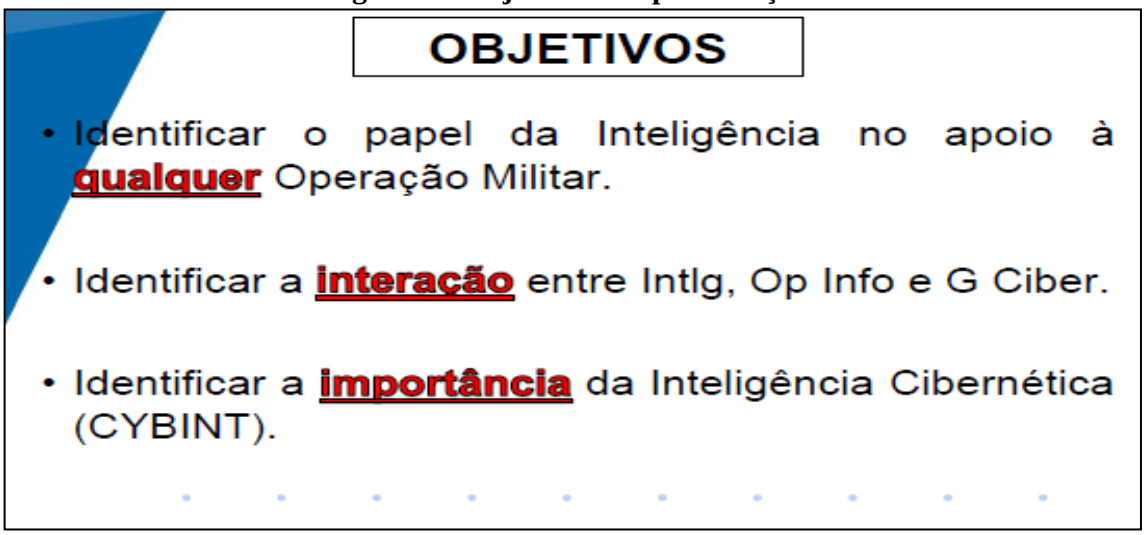
Armadas é um privilégio, uma vez que é o único estabelecimento de ensino de inteligência das Forças Armadas.

Estive na Colômbia durante um ano, período em que me aprofundei a respeito de inteligência cibernética, que atua basicamente no nível estratégico. A Escola de Inteligência do Exército está em sua fase inicial. Há dois anos que a Escola forma militares especializados em inteligência cibernética.

Vocês perceberão que não é fácil formar um militar com essas características, porque ele não nasce com o DNA desejável para aquela atividade. Mas, graças a Deus, essa juventude que vem por aí já tem o DNA requerido para esse tipo de ação. Ou seja, selecionar e preparar militares voltados para a inteligência cibernética não é uma atividade fácil, pois é difícil encontrar uma pessoa que tenha esse perfil. Por quê? Porque não se encontrar e capacitar um militar especializado ou uma pessoa especializada que possua essas características, o sistema poderá ser comprometido. Tem também o quesito da seleção de recursos humanos, da vaga no sistema, etc.

A contrainteligência é inerente ao militar. Em qualquer apresentação projetada por comerciais de inteligência, aparece algo relativo à contrainteligência como alerta. Há que se ter um cuidado quando ouvir a expressão: “Joga na nuvem, pega na nuvem". Na verdade, a nuvem é apenas o computador de outra pessoa. Tudo o que é colocado na nuvem, está no mundo virtual. Fica apenas o registro da nossa mensagem de inteligência. Dito isto, a figura a seguir apresenta os objetivos da nossa apresentação para o dia de hoje:

Figura 2 - Objetivos da apresentação



Fonte: o autor, 2019.

Pobre do chefe que não dá valor a essa atividade. Em algum momento vai se arrepender. Porque a inteligência é assim. Uma hora ele pode estar no “dez” e em fração

de segundos pode ir para o "zero". Dessa forma, é importante identificar a interação existente entre a inteligência, as operações de informações e a guerra cibernética. Para isso, serão tratadas algumas ideias simples e básicas sobre a importância da inteligência cibernética. Não há dúvidas de que a inteligência cibernética é muito importante. É a quarta fonte da atividade de inteligência: é a caçula. Mas que veio para ficar e não tem para onde correr. Vamos gravar essa ideia.

Essas são as gerações da guerra: a 1ª geração, a 2ª geração, a 3ª geração e a 4ª geração. Atualmente estamos vivendo o conflito da 5ª geração, que é justamente o conflito de amplo espectro:

Figura 3 - As Gerações da Guerra

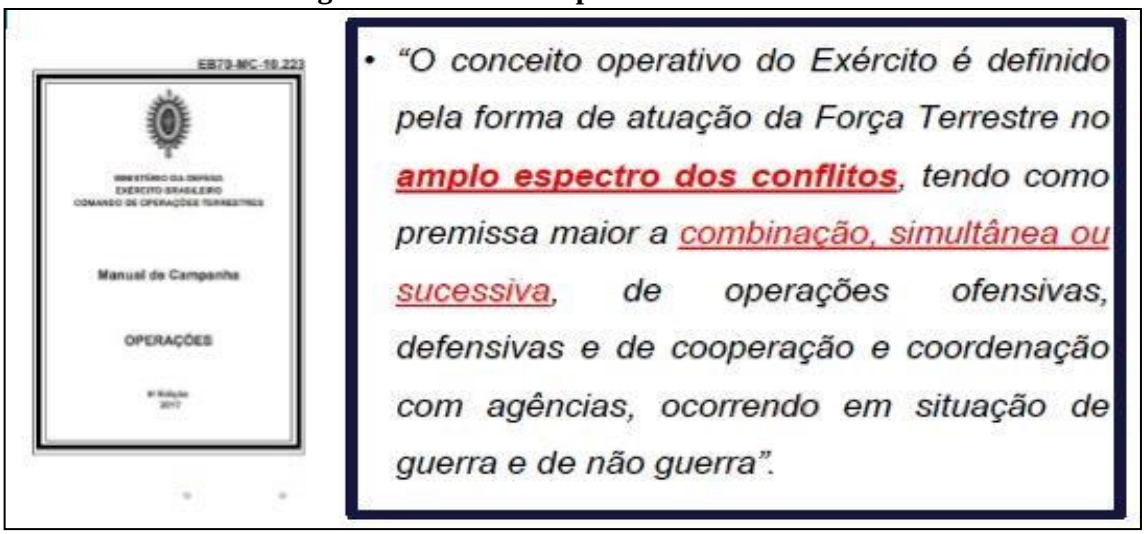
Fonte: o autor, 2019.

As características do combate atual são as seguintes: combate em áreas edificadas, emprego de pequenas frações, ameaças de difícil identificação, presença de atores diversos, a importância das considerações civis, operações conjuntas e/ou combinadas e as ameaças cibernéticas.

O Brasil está absolutamente inserido no que acontece hoje no combate, no conflito de quinta geração, de amplo espectro. Num conflito em que não existe mais a definição indireta. De um lado é retaguarda, do outro lado é o limite direito, do outro lado é o limitre esquerdo, etc. Essa formatação maravilhosa não existe mais. Agora é uma Brigada defendendo uma área importante e atacando em outra direção. Esse é o conflito atual.

Alguns anos atrás era diferente. Mas, com a era da informação que nós estamos vivendo, esse é o cenário que se apresenta. Com isso, as ameaças cibernéticas no ambiente virtual complicam ainda mais, pois elas eliminam as fronteiras, interligando todos os atores, ou seja, é um ambiente que não consegue dimensionar. Olha o conceito operativo do Exército Brasileiro que está no manual de operações:

Figura 4 - Conceito Operativo do Exército



Fonte: o autor, 2019.

Esse conceito possibilita uma gama variada de possibilidades: operações ofensivas, defensivas, combinação simultânea, sucessiva, seja lá o que for. Essas operações podem estar acontecendo ao mesmo tempo atualmente. No que concerne ao Brasil, percebe-se a participação de vários órgãos, como o Banco do Brasil, a Receita Federal e a Polícia Federal em operações cibernéticas. Um verdadeiro "balaio de gato", mas não tem para onde correr. É necessário se adaptar a essa realidade.

2. Desenvolvimento

O que é inteligência? É um conjunto de atividades e tarefas técnico-militares em caráter permanente, com os objetivos de produzir conhecimentos de interesse para os Comandantes e seus Estados-Maiores (de todos os níveis) e para proteger conhecimento específico. Esses são os dois ramos da atividade de inteligência: 1) Inteligência; e 2) Contrainteligência. A atividade de inteligência é única. Não pode separar a inteligência de combate, da inteligência de cidadão.

O Exército Brasileiro está atravessando uma fase de transformação. Viveu-se um período em que o governo militar precisou muito da inteligência voltada para a atividade institucional. Por outro lado, a atividade de inteligência de combate, que vinha da 2ª Guerra Mundial, ficou congelada. Atualmente a instituição está retirando a inteligência de combate da "geladeira" para que a mesma chegue ao mesmo nível da inteligência institucional. Mas são atividades diferentes? Não, muito pelo contrário, são muito semelhantes. Mas, a inteligência institucional vai desaparecer? Não vai. Ela está mais viva do que nunca. Mas ela é útil? Claro que é util. Ela tem emprego? Claro que tem. Acabou-se de falar acerca do conflito de 5ª geração. Mais útil do que nunca.

De acordo com o manual: Inteligência Militar Terrestre, as disciplinas de inteligência estão classificadas de acordo com a natureza das fontes ou do órgão de obtenção que a explora. Nesse rol, há a inteligência humana, a inteligência de imagem, a geointeligência, a inteligência de aquisição de alvos, a inteligência de fontes abertas, a inteligência de sinais, a inteligência cibernética, a inteligência tecnológica, a inteligência artificial e a inteligência médica:

Figura 5 - Disciplinas de Inteligência

Fonte: o autor, 2019.

E quais são os ambientes de emprego da inteligência? São 3 ambientes: o ambiente de obtenção, que é o local onde os dados são obtidos (destaque para a inteligência cibernética, de imagem e de sinais); o ambiente de análise, local onde estão localizados os analistas; e o ambiente de comando e controle, local onde está o Comandante e seu Estado-Maior. Esses são os ambientes que a inteligência do Exército Brasileiro trabalha para prestar assessoramento aos Comandantes e seus Estado-Maiores em todos os níveis, a fim de que os mesmos possam cumprir suas missões.

Auxiliado por outras agências, o Sistema de Inteligência do Exército Brasileiro está inserido no Sistema de Inteligência de Defesa, que por sua vez, está inserido no Sistema de Inteligência Nacional.

Os meios de obtenção atuam no espaço de batalha e no ambiente operacional como sensores de dados, identificando as ameaças e as oportunidades existentes (podem ser especializados ou não especializados). O ambiente operacional comporta a dimensão física, a dimensão humana e a dimensão informacional, pelo que se torna muito mais amplo do que aquele simples espaço físico que se tinha há pouco tempo atrás.

Trabalhando num ambiente com oportunidades e ameaças, a inteligência vai assessorar os seus Comandantes. A inteligência é uma função de combate e quando se

fala em combate, é no amplo espectro. É nesse ambiente que a inteligência opera. As atividades da função de combate inteligência no amplo espectro são as seguintes: 1) produzir conhecimentos continuamente em apoio ao planejamento da Força; 2) executar ações de inteligência; reconhecimento, vigilância e aquisição de alvos (IRVA); 3) apoiar a obtenção da consciência situacional; 4) apoiar a obtenção da superioridade da informação; e 5) apoiar na busca de ameaças.

O que orienta e dirige as operações de inteligência? Qual o papel dela em qualquer operação? O papel dela é orientar as ações, potencializar os resultados e minimizar os custos. Por isso que o trabalho de inteligência é meticuloso, porém tenham a certeza de que trabalhar sem ela é muito pior.

Todas as operações de informações atuam de forma integrada com as capacidades relacionadas à informação (CRI) e têm por objetivo informar e influenciar grupos e indivíduos para afetar o ciclo decisório do oponente, talvez até protegendo o nosso ciclo decisório. Somente a atuação integrada e sincronizada das operações de informação pode contribuir efetivamente para o sucesso da missão.

Figura 6 - Capacidades Relacionadas à Informação das Operações de Informação

Fonte: o autor, 2019.

Nos dias atuais, nota-se a existência de cinco CRIs que atuam no contexto das operações de informação: inteligência, comunicação social, operações psicológicas, guerra eletrônica e guerra cibernética.

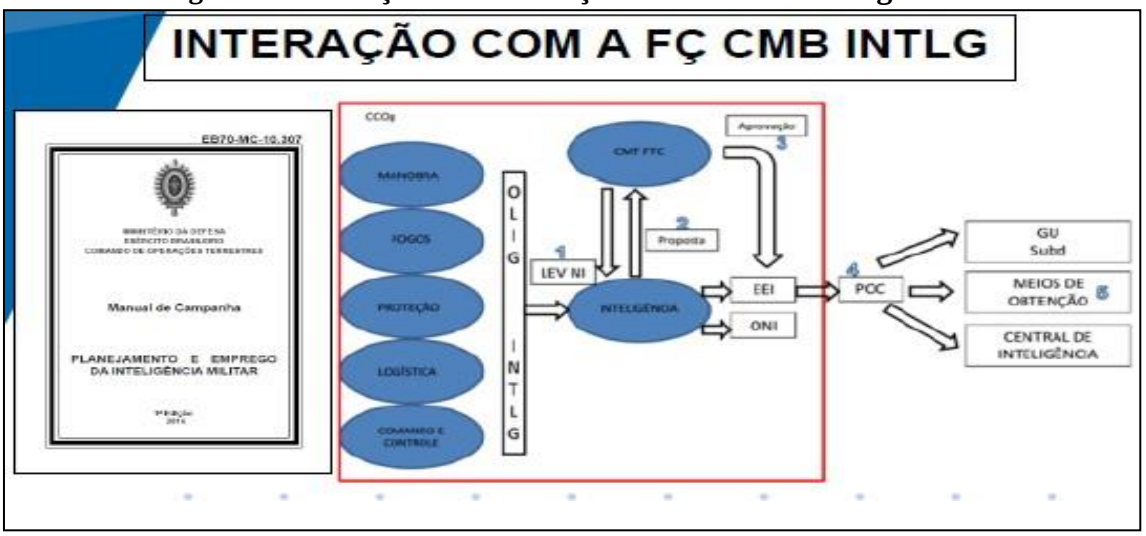
Será que a guerra cibernética faz isso, faz aquilo? E as operações de informação propriamente dita? As duas podem atuar em prol de um objetivo bem definido?

Figura 7 - Guerra Cibernética

Fonte: o autor, 2019.

Observem um aspecto interessante na definição de guerra cibernética: uso ofensivo e defensivo de informação e sistemas de informação para negar capacidade de comando de controle ao adversário. Dessa forma, a inteligência cibernética estabelece um vínculo com a guerra cibernética. Operações militares abrangem ações cibernéticas, como proteção cibernética e os ataques cibernéticos de exploração cibernética:

Figura 8 - Interação com a Função de Combate Inteligência

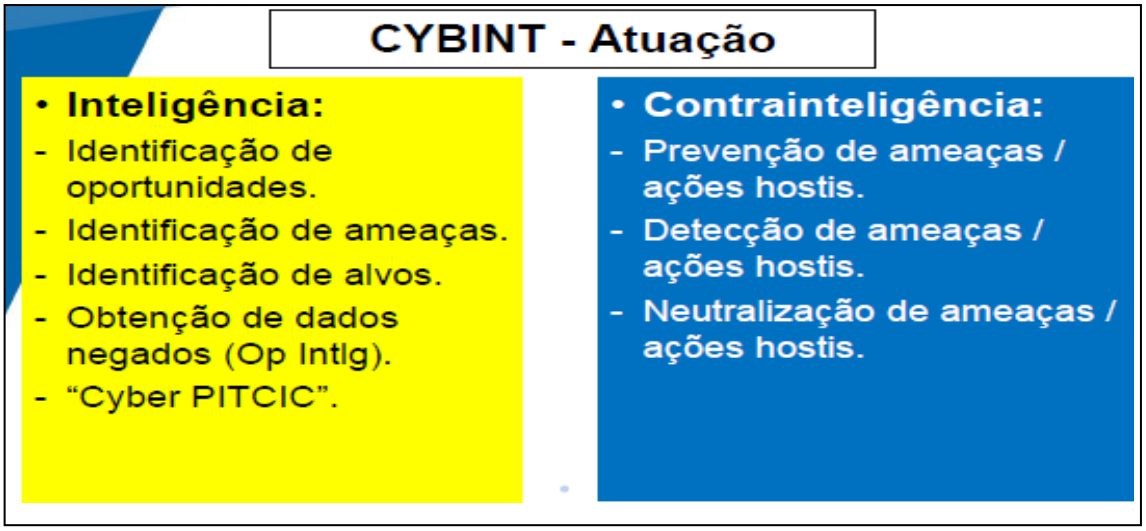


Fonte: o autor, 2019.

A figura anterior mostra que a inteligência atua em todas as funções de combate levantando as necessidades de inteligência que vem justamente do Comandante e de seu Estado-Maior. Após isso, é gerado o plano de obtenção do conhecimento. A partir daí, especializados ou não especializados, devem trabalhar para conseguir os dados necessários (protegidos ou não), que atendam às necessidades da inteligência e os elementos essenciais de inteligência inseridos no plano de obtenção do conhecimento. Todos têm que trabalhar. Desde o soldado mais moderno até o chefe mais antigo.

Por definição, a inteligência é elaborada a partir de dados, protegidos ou não, obtidos no espaço cibernético. Dado que não é protegido, é aquele que para obter é necessário em algum momento transpor um obstáculo. E para isso, pode utilizar os meios que forem necessários para que aquele dado seja buscado no espaço cibernético. A inteligência cibernética pode atuar da seguinte forma.

Figura 9 - Atuação da Inteligência Cibernética



Fonte: o autor, 2019.

3. Conclusões

A inteligência é uma função de combate. É um princípio basilar. Se uma pessoa quer começar a construir uma ideia, precisa começar a construir a partir daí.

Dessa forma, entende-se que a inteligência é uma função de combate que se destina a satisfazer as necessidades de inteligência dos Comandantes e de seus Estados-Maiores em todos os níveis, subdisiando o planejamento e a condução de todas as operações militares. A inteligência, como função de combate, não está apenas vinculada às operações de informações. Pelo contrário, ela procura responder as necessidades de todas as células do Estado-Maior indistintamente, organizando, priorizando, direcionando-as para os sensores mais adequados.

Muito obrigado.

Mais uma vez, agradeço pela disponibilidade. Tudo de bom!

A CIBERNÉTICA SOB A PERSPECTIVA GEOPOLÍTICA

Ricardo Borges Gama Neto*

1. Introdução

Boa tarde a todos. É um prazer estar na Escola de Comando e Estado-Maior do Exército participando do XXI Ciclo de Estudos Estratégicos.

Sem muitas delongas, a primeira coisa que coloco é que a minha preocupação hoje com a cibernética tem a ver com questões que são modernas. Dessa forma, o primeiro aspecto se refere à geopolítica. Sob a perspectiva geopolítica, a cibernética é um espaço completamente aberto e que não tem fronteiras. Por que é importante? Porque a geopolítica é um assunto um pouco mais do que isso, na medida em que há geopolíticas econômicas e todas elas quiseram acabar com a produção de computadores simplesmente para ficar de igual para igual. É um esporte.

A segunda coisa tem a ver com o conceito de guerra cibernética, mais precisamente de inteligência artificial. Quais são os dois problemas da cibernética em gera nos dias atuais? A resposta passa pelas pessoas e pelos equipamentos. O lado mais fraco da guerra cibernética é o equilíbrio. Você sabia que não pode usar *pendrive* de casa dentro de uma usina nuclear? A legislação americana diz que nenhum oficial ou nenhum político importante pode usar *email*. A *Hilary Clinton* utilizou o *email* particular dela e todos sabem o que ocorreu. Então, o indivíduo é o principal problema da guerra cibernética. Outro problema é o *software*.

Qual a possível solução para isso? O princípio é você poder retirar o indivíduo e elaborar estratégias de ataque ou utilizar inteligência artificial para diminuir ou até mesmo eliminar as chances de ataque cibernético. A inteligência artificial ajuda no banco de dados, o qual pode ser utilizado na elaboração de uma estratégia. Colete informação, depois disso monte uma estratégia.

2. Desenvolvimento

Vou fazer uma pergunta para a assistência: Quem já pegou o seu telefone e ligou para a esposa para perguntar se ela queria viajar? Perceberam que aparece um pacote de viagem quando você vai ao navegador, ou simplesmente ao *facebook*? Perceberam que

* Doutor em Ciência Política e Professor Adjunto IV da Universidade Federal de Pernambuco.

quando você dá um *like* num telefone, rapidamente você está recebendo a propaganda desse mesmo telefone? Isso é inteligência artificial.

Estou falando num nível em que a guerra cibernética se torna algo quase que independente. Os Comandantes militares querem que a máquina faça o serviço. A ideia principal é tirar a possibilidade de erro.

Posso estar enganado, mas me parece que toda guerra cibernética começa com matéria de engenharia social, que está presente no dia a dia de todas as pessoas. O que eu vou fazer é tornar isso mais complexo. Vamos dizer que eu queira *hackear* uma usina hidrelétrica. Eu não sei fazer funcionar, mas eu posso imaginar o que eles deveriam comprar. Dessa forma, eu vou vasculhar a *internet* buscando pessoas que, teoricamente, trabalham numa empresa hidrelétrica. Depois, eu posso fazer o quê? Eu posso simplesmente tentar invadir o *site* da Receita Federal e tentar coletar os CPF dessas pessoas. E, depois disso, tentar utilizar *emails* e *links* para infectar esse alvo. Uma hora, essa pessoa vai dar um clique e o seu computador será infectado. Quando você for pegar o seu *pendrive* particular e levar para a empresa, as informações da empresa serão coletadas.

Você não tem somente uma equipe atuando. Pelo contrário, empregam-se várias equipes diferentes com o propósito de se montar a estratégia. Uma colhe a informação, a outra analisa a informação e a outra emite uma resposta. Eu vou ter aqueles analistas de gerente que vão decidir o que fazer, como e quando. Em longo prazo, as mesmas te deixam cada vez mais automatizado. Vai acabar com a ação humana? Não, mas vai ser obrigado a ter especialistas.

É interessante como hoje em dia, alguns países coletam os seus *cibersoldados*. Alguns países não têm dificuldade de formar *cibersoldados,* como exemplo Israel. Como que Israel procura seus *cibersoldados*? Procuram no ensino médio. Hoje em dia há uma competição na busca de um *cibersoldado*. Alguns países, como a Coreia do Norte, começam a treinar seus *cibersoldados* no nível fundamental. Outro exemplo é a China, que buscam seus *cibersoldados* no ensino médio, atuando com base no rendimento dos alunos em matemática e computação. Em suma, alguns países têm dificuldades e outros não têm em coletar seus *cibersoldados*.

E os países que têm maior número de *cibersoldados* investem pesado em tecnologia. O ambiente *ciber* custa dinheiro? Custa muito dinheiro. É um mito aquela imagem que as pessoas plantavam que esse negócio era apenas ficar sentado atrás do computador de noite, com óculos grandes, comendo batatinha frita e tomando café. Não

é assim, *ciberdefesa* é muito custoso. E, infelizmente, a tendência é custar mais caro ainda porque para ter boas máquinas custa dinheiro, da mesma forma que ter bons profissionais para serem treinados custa muito dinheiro. Ou seja, para você manter um bom *cibersoldado*, vai ter que pagar muito bem para ele.

Dessa forma, entende-se que o desafio principal é tentar entender como a inteligência artificial pode ser utilizada no ambiente *ciber* num nível cada vez mais avançado. Os Comandantes militares decidem e os programas fazem os serviços. Há um programa que foi feito contra um alvo muito específico, só que ele se espalhou de tal maneira num gaseoduto na Índia, que saiu travando máquina em outros países da região, vindo a atacar fortemente setores do Irã, Índia e Paquistão.

Existem casos semelhantes em que se tentaram atingir determinado objetivo, mas quando se colocou em prática, perdeu-se o controle e acabou indo para outros caminhos. Um desses casos ocorreu numa universidade, onde foi feito uma experiência em sala de aula e terminou fazendo estragos gigantescos. Um aluno resolveu perguntar: "Eu posso driblar um antivírus?" Passou pela sala de aula, brincando com os colegas e alguém botou na rede da Universidade, que logo se espalhou. E foi necessária a intervenção da universidade junto aos fabricantes das máquinas para resolver o problema. Fato é que demorou um tempo até que os próprios fabricantes do *software* fizessem uma correção por uma coisa que eles nunca haviam pensado.

Há várias questões que podem ser colocadas nesse tipo de estrutura. Voltando um pouco a questão da *ciberinteligência*. Talvez a *ciberinteligência* seja um pouco além da ideia da inteligência humana. Torna-se necessário começar a pensar no sistema de automação inteligente também.

A *National Security Agency* (NSA) faz coleta de informação e informa. Mas e as instituições não militares, os bancos, as centrais de eletricidade, de Telecomunicações? É necessária toda uma legislação para você trabalhar na área não militar. A partir da conta de um funcionário, eu posso fazer um ataque numa área não militar e danificar os sistemas das infraestruturas críticas. Ou seja, é imperioso passar na cibernética como um sistema que envolve o setor militar e o setor civil.

A Teoria Clássica dos Sistemas, que monta o sistema, afeta todos os outros. Para se pensar em cibernética, há que se voltar um pouco à Teoria dos Sistemas. A alteração de um texto impacta em todos os outros. O impacto da tecnologia nessas áreas vai poder influenciar todas as outras. Dessa forma, nota-se que algumas infraestruturas têm sido incorporadas à ideia de defesa num guarda-chuva maior.

A tendência em longo prazo é que haja cada vez mais a ação das máquinas, ou seja, da robotização no sistema de defesa. Se alguns anos atrás, uma instituição tinha quatro soldados, hoje ela conta com apenas três, sendo um substituído por robô. As instituições militares possuem cada vez mais robôs atualmente. Nos navios, boa parte das classes que anteriormente eram manuais, hoje estão robotizadas. Quanto mais automatiza, maior o risco de sofrer ataques.

Eu me lembro da história de um submarino inglês que, um belo dia no mar, teve a ideia genial de economizar 15 mil libras esterlinas e apertou um botão, ação que travou todo o sistema. Depois, teve o caso da Força Aérea Francesa, onde um militar francês colocou um *pendrive* com vírus para ouvir música no sistema, vindo a contaminar e deixar parado o mesmo, porque ninguém sabia o que ia acontecer se aquele vírus passasse para o sistema de navegação naval. Então, a tendência dos próximos anos é abrir brechas cada vez maiores em todo o sistema de defesa, haja vista a tendência de automatização dos processos e da substituição do homem por robôs.

Eu fico me lembrando da Guerra Nuclear, quando tinha um jogo de computador e no contexto do jogo, havia uma pergunta: Você quer jogar uma guerra nuclear? E aí a pessoa dizia: "Quero". Essa é uma resposta. Só que ela não tinha a menor ideia de que o jogo era de verdade.

Por que essa mensagem é atual hoje em dia? A primeira coisa é que a guerra cibernética não consegue ter a ideia da dimensão física. O segundo aspecto recai em fatores ligados ao investimento, treinamento e tecnologia. E, mesmo com mais treinamento, provavelmente haverá problemas operacionais. O terceiro aspecto a se pensar e que também continua sendo um fator importante é a defesa. Entende-se que a cibernética tem que trazer o sistema civil junto ao sistema de defesa. Não dá para você imaginar tudo aqui sem pensar nas infraestruturas críticas: bancos, água.

Quando se estuda a hsitória das últimas guerras, percebe-se claramente a atuação da guerra cibernética no contexto das operações militares. Por exemplo, a guerra da Crimeia começou com um apagão elétrico e depois houve um apagão no sistema de telefonia, que desorganizou completamente o Governo e o Exército Ucraniano.

Na década de 1990, ocorreu outro exemplo de ataque cibernértico na Guerra do Iraque. Os norte-americanos entraram na rede do sistema de defesa aéreo iraquiano e danificaram o funcionamento dos radares iraquianos, fato que fez toda a diferença nesse conflito, uma vez que as aeronaves militares dos países aliados voavam tranquilamente a uma altitude de quinze, doze mil metros sem serem molestadas pelo fogo iraquiano. Se

isso foi possível na década de 1990, imagina a possibilidade das coisas que podem ser feitas nos dias atuais. E isso não é um crime, eu estou falando de defesa. Crime é outra coisa: é um *hacker* que rouba a senha do *whatsapp*. Estou falando que uma pessoa é treinada (por um Estado-Nação) para fazer isso. Ou seja, para buscar vulnerabilidades no sistema dos outros.

3. Conclusões

Como conclusão, nota-se que o mais interessante hoje na cibernética é que não há um regime internacional ou leis ou regras que regulamentem os processos e ações que podem ser executadas. E dessa forma, todo mundo espiona todo mundo. Quem não espiona é quem não tem capacidade técnica para espionar. Todo mundo espiona todo mundo. Todo mundo busca as fraquezas de todo mundo. Enquanto você não tiver um ordenamento juridico internacional que dite regras gerais, isso será possível.

A única coisa que pode ser feita é investir, treinar e partir para a ofensiva. Por que ofensiva? Atacarmos a nós mesmos, buscando fragilidades. É a única coisa que dá para fazer. Criar, porque não se consegue fazer defesa sem fazer ataque. Uma das falhas é imaginar que pode ter a defesa cibernética simplesmente pensando em segurança, sem atacar.

Um país só consegue imaginar a defesa se você souber atacar. Se não souber o que buscar, onde buscar e como buscar, não se consegue defender. Se imaginarmos que vai apenas se defender, não vai. É aquela história de jogador de futebol que fica só se defendendo. Uma hora a bola vai entrar. É isso que eu tinha que falar para vocês.

Muito obrigado!

PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS CONTRA ATAQUES CIBERNÉTICOS

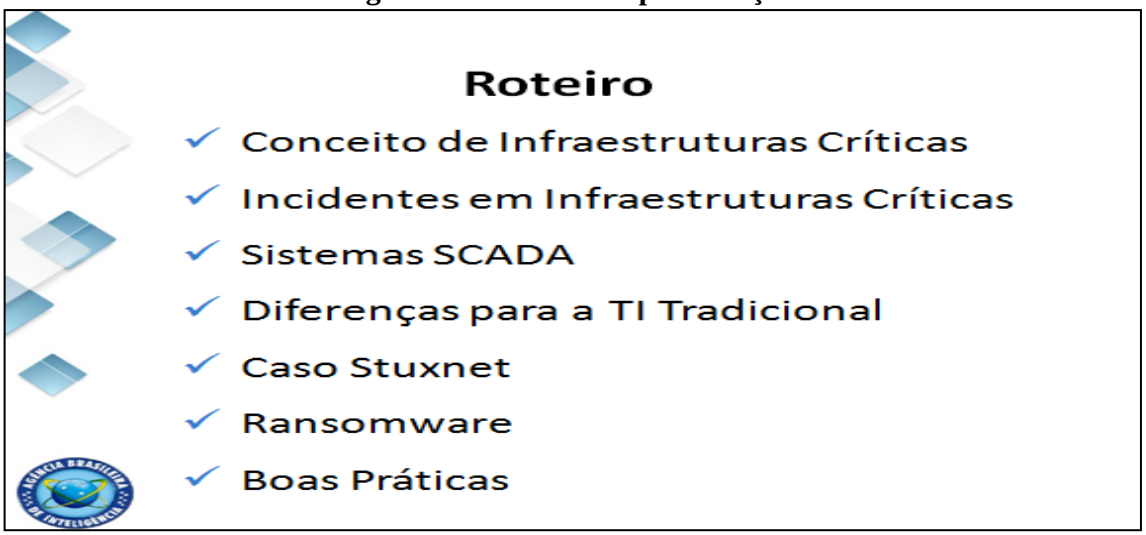
Alisson Campos Raposo*

1. Introdução

Bom dia a todos.

Meu nome é Alisson Raposo e trabalho na Agência Brasileira de Inteligência (ABIN). É uma satisfação estar em nome da Agência Brasil de Inteligência na Escola de Comando e Estado-Maior do Exército (ECEME), que é um local onde se debate conhecimentos bastante interessantes. Eu tive uma passagem bastante interessante na Escola Superior de Guerra (ESG), ocasião em que tive a oportunidade de conhecer a metodologia e a forma de analisar das instituições e das escolas militares.

Figura 1 - Roteiro da apresentação



Fonte: o autor, 2019.

Hoje, eu acredito que uma das maiores pragas que nós temos e que diversas instituições foram atingidas diz respeito à contaminação de vírus em sistemas computacionais. Dessa forma, minha intenção é que ao longo da apresentação sejam repassadas algumas boas práticas que podem ser adotadas.

2. Desenvolvimento

A atribuição institucional da ABIN em trabalhar nessa área vem da Lei 9.883, de 07 de dezembro de 1999, em seu artigo 4º, conforme a figura a seguir:

* Oficial de Inteligência da Agência Brasileira de Inteligência.

Figura 2 - Atribuição institucional

Fonte: o autor, 2019.

Em 2008, tive a satisfação de fazer parte dos primeiros grupos de trabalhos voltados para a segurança e infraestrutura crítica no Gabinete de Segurança Institucional (GSI). Nessa época, iniciou-se o mapeamento das infraestruturas críticas, da mesma forma que foram tomadas as primeiras medidas para a proteção das infraestruturas, com a ABIN exercendo um papel bem interessante no desenvolvimento de metodologia.

As infraestruturas críticas são os sistemas que compõem a infraestrutura de um Estado, para os quais a continuidade da operação é tão importante que a perda, interrupção significativa ou degradação dos serviços poderia ter graves consequências econômicas, polítcas e, sobretudo, sociais. A partir dessa definição podem-se identificar diversas instituições que se enquadrariam como infraestruturas críticas. Destaque a parte deve ser dado para a questão da interrupção das infraestruturas críticas que são projetadas para funcionar sem interrupção durante um período prolongado.

O primeiro caso de infecção nos sistemas computacionais de estruturas críticas ocorreu em janeiro de 2003, ocasião em que a planta nuclear de *Davis-Besse* foi infectada pelo vírus: *Worm "Slammer"*. Esse vírus causou a paralisação, por quase cinco horas, dos sistemas computacionais da usina e causou a interrupção do computador de processos da planta da respectiva usina por seis horas.

O segundo caso dessa natureza ocorreu em agosto de 2005, nas plantas da empresa automobilística *Daimler-Chrysler*. Neste caso, 13 plantas norte-americanas foram desligadas por um simples vírus *Worm*. A consequência disso foi a paralisação de 50 mil trabalhadores e um prejuízo estimado em 14 milhões de dólares. A causa desse incidente provavelmente foram alguns códigos maliciosos introduzidos num caminho secundário na rede, ou seja, apesar de *firewalls* profissionais instalados entre a *internet* e a rede da

empresa, o *Worn* encontrou uma forma de entrar no sistema de controle.

Outro caso semelhante ocorreu em agosto de 2006 nos Estados Unidos da América (EUA). Nessa época, operadores da planta nuclear de *Browns Ferry* no Tennessee, tiveram que desligar o reator da usina. O vírus *worm* parou as bombas de recirculação dos reatores 3A e 3B. As principais causas foram atribuídas ao excessivo tráfego entre dois produtos de controle de diferentes fabricantes e aos controladores das conexões *internet* para as redes ICS (*Integrated Computer System*) das plantas. A planta ficou parada por dois dias e o prejuízo estimado ficou em 600 mil dólares.

Um caso famoso ocorreu na Estônia em 2007. Nessa ocasião, a infraestrutura da Estônia foi atacada durante três semanas. Tais ataques foram atribuídos aos *hackers* da Rússia, que realmente colapsaram diversas instalações e infraestruturas da Estônia. Desde então, tem se tornado cada vez mais comum a ocorrência desses ataques:

Figura 3 - Casos de ataques cibernéticos

Fonte: o autor, 2019.

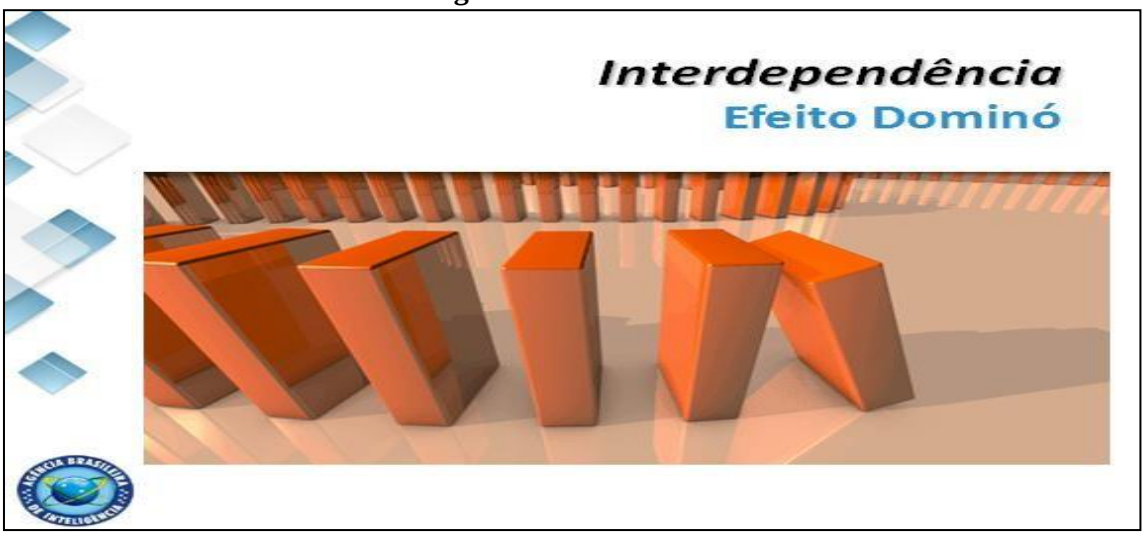
Quando se analisa o ataque e seus efeitos na infraestrutura, nota-se o transtorno que o mesmo causa na respectiva infraestrutura. Imagine as interdependências existentes entre as estruturas de uma planta de geração de energia elétrica. Se uma delas falhar, vai afetar todas as outras.

Dessa forma, a questão da interdependência foi um grande desafio para a ABIN quando participava desse grupo de estudo. De certa forma, não havia maiores complexidades quando as estruturas eram analisadas por sistema separadamente. Mas quando as mesmas eram analisadas, considerando as interdependências existentes entre elas, a questão ficou bem mais complicada.

Uma estrutura que é derrubada vai levar as outras junto com ela, gerando o famoso efeito dominó, a menos que haja uma estrutura com resiliência para intemrromper essa

sequência de ataques ou interromper esse *crash* em sequência:

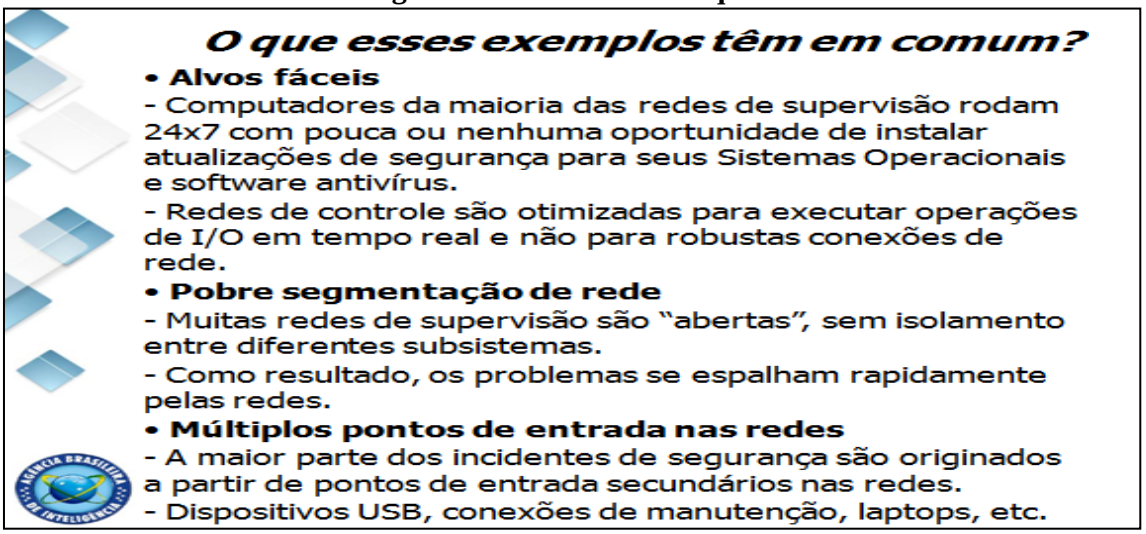
Figura 4 - Resiliência



Fonte: o autor, 2019.

De toda sorte, os exemplos apresentados apresentam aspectos em comum:

Figura 5 - Motivos dos ataques



Fonte: o autor, 2019.

A maior parte das infraestruturas críticas é controlada por um conjunto de computadores chamados SCADA (*Supervisory Control and Data Acquisition Systems)*, que são compostos por Sistemas de controle de processos, Sistemas de controle distribuídos (DCS), *Programmable Logic Controllers* (PLC), *Inteligent Electronic Device* (IED) e *Human Machine Interface* (HMI). De alguma forma, eles podem ser atingidos por um ataque *hacker*.

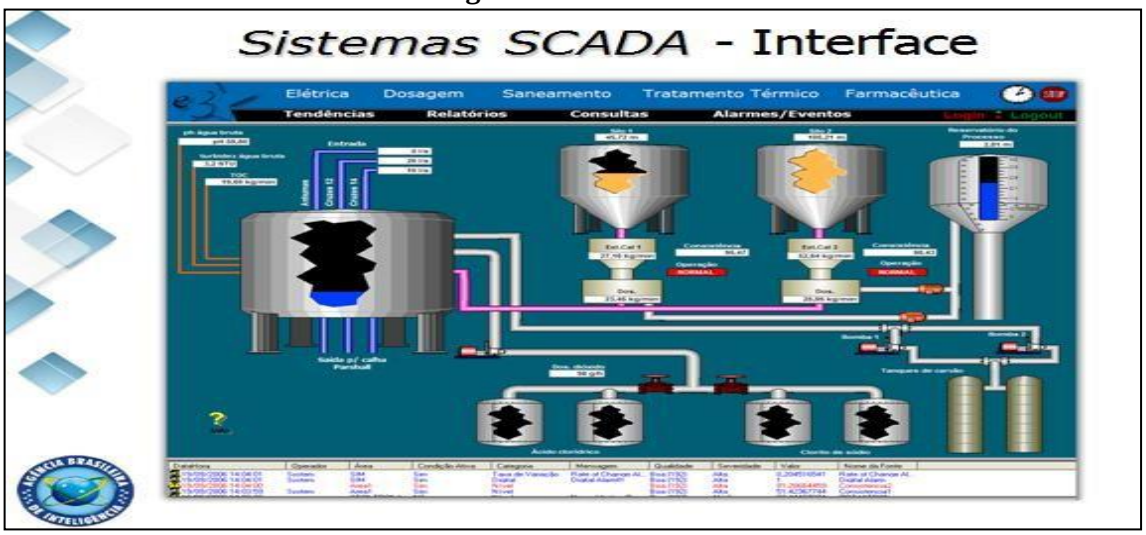
Na TI tradicional, a integridade dos dados e a proteção de ativos são a prioridade principal. Em automação, a segurança da planta é o mais importante. Os Sistemas de Supervisão são projetados para terem altíssima disponibilidade, ou seja, eles são projetados para funcionarem por um longo período.

Figura 6 - Sistemas SCADA x TI

Fonte: o autor, 2019.

O tripé da segurança da informação é confidencialidade, integridade e disponibilidade. Constata-se uma inversão de prioridades quando se analisa as redes industriais e as redes de TI tradicional. Na TI tradicional, a ordem de prioridade é a seguinte: 1) confidencialidade; 2) integridade; e 3) disponibilidade. Na automação industrialo caminho é inverso: 1) disponibilidade; 2) integridade; e 3) confidencialidade. A interface homem-máquina de uma rede industrial é algo mais ou menos assim:

Figura 7 - Interface

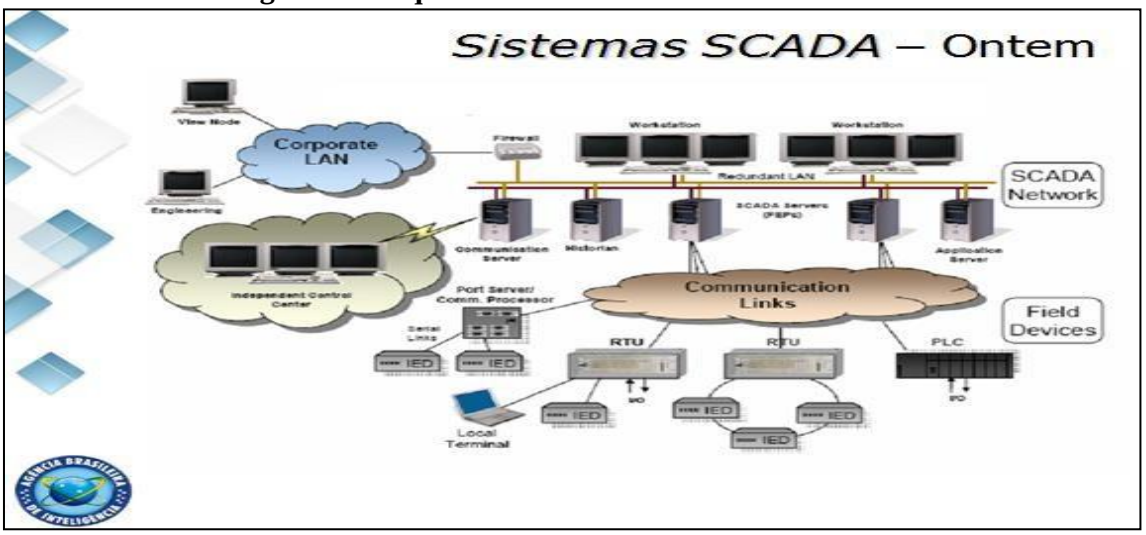


Fonte: o autor, 2019.

Como eram essas redes antigamente? Essas redes foram concebidas na década de 1970, época que não havia problema com vírus. Não havia preocupação com acessos externos via *internet*, por exemplo. Esses sistemas eram considerados intrinsecamente seguros, pois eram isolados do mundo exterior e a partir dessa concepção, eles foram construídos e desenvolvidos. Só que as redes corporativas foram mudando e ao longo dos anos os equipamentos foram sendo conectados à rede industrial e à rede corporativa.

Dessa forma, as vulnerabilidades que chegam via rede corporativa podem ser atingidas na rede industrial porque ela não foi projetada para isso.

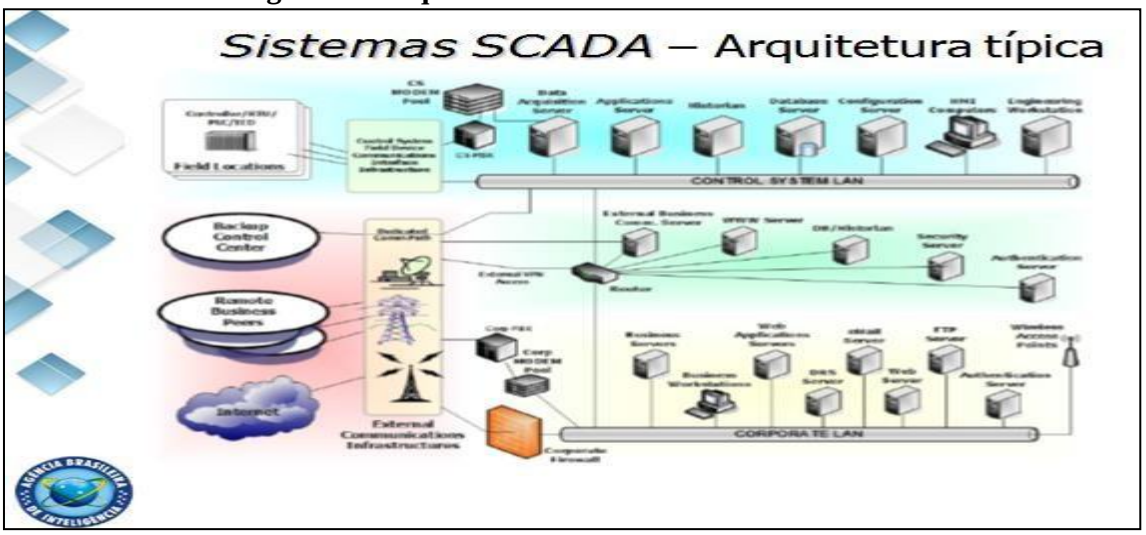
Figura 8 - Arquitetura inicial dos sistemas SCADA



Fonte: o autor, 2019.

Essa era a situação naquele tempo, hoje a coisa mudou bastante. Ainda existe a rede industrial e com diversas formas de acesso externo. No entanto, basta ter um *firewall* da rede corporativa para inibir de alguma forma o acesso do mundo exterior a essa rede. A figura a seguir apresenta uma arquitetura típica dos sistemas SCADA:

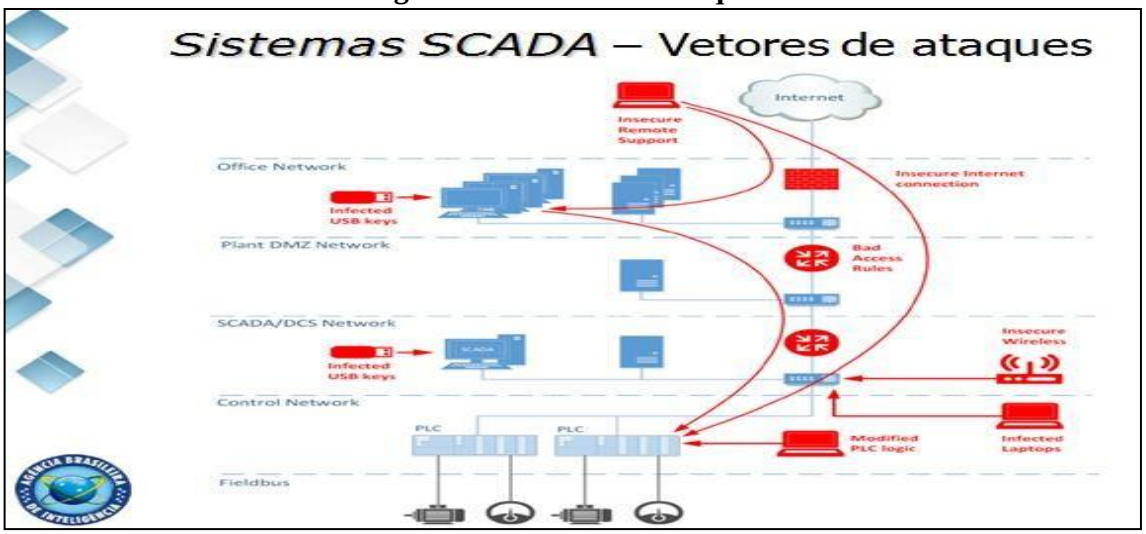
Figura 9 - Arquitetura atual dos sistemas SCADA



Fonte: o autor, 2019.

Existem diversas formas para que um ataque externo chegue até a uma rede. Desde a forma remota a rede (um *pen drive* infectado que é conectado) e vai passando pelo *firewall* na rede interna diretamente, ou uma rede de *wi-fi* insegura, ou um *laptop* infectado, etc. Ou seja, há uma série de caminhos possíveis para um ataque cibernético chegar até a rede corporativa, conforme destacado a seguir:

Figura 10 - Vetores de ataques



Fonte: o autor, 2019.

Na sequência, são comparados alguns itens de segurança utilizados na tecnologia da informação e nos sistemas de controle:

Figura 11 - Itens de segurança

ITEM DE SEGURANÇA	Na Tecnologia da Informação	Nos Sistemas de Controle
Antivírus	Amplamente utilizado	Difícil ou impossível implantação
Suporte da tecnologia	2 a 3 anos, com fornecedores diversos	Acima de 20 anos, com um único fornecedor
Terceirização	Amplamente utilizada	Utilizada, mas muito especializada
Aplicação de patches	Agendamento regular	Muito rara
Troca de gestão	Normal	Complexa
Tempo de conteúdo crítico	Normalmente atrasos são aceitos	Atrasos são inaceitáveis
Disponibilidade	Normalmente atrasos são aceitos	24 x 7 x 365 (contínua)
Consciência de segurança	Moderada/alta, tanto no setor público como no privado	Pobre, exceto para segurança física
Teste ou Auditoria de Segurança	Parte de uma boa Política de Segurança	Raros ou ocasionais
Segurança Física	Segura (servidores, salas-cofre etc.)	Remota / Automatizada

Fonte: o autor, 2019.

Algumas formas de se fazer os ataques a sistemas de SCADA: 1) o primeiro é o *Loss of View*: consiste na perda de visão. É quando na interface homem-máquina o operador não possui a visão do que está ocorrendo. Se o sistema não for automatizado o suficiente para permitir que a operação ocorra de forma normal sem a intervenção do operador, será bastante complicado.

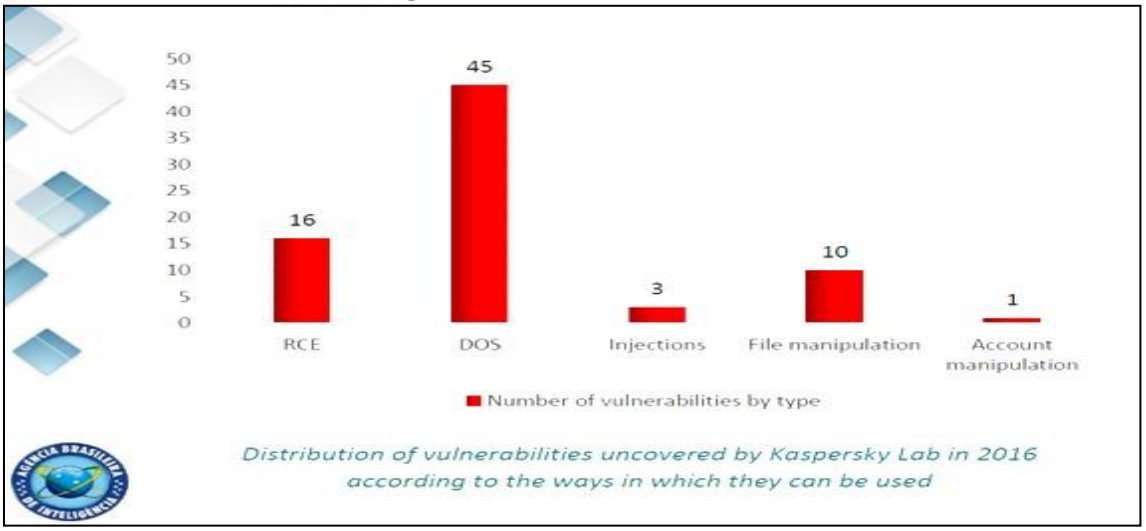
O segundo tipo de ataque é a *Manipulation of View*: consiste na manipulação da visão. É quando o operador está recebendo uma informação visual diferente do que está ocorrendo. No *Stuxnet* tivemos esse tipo de situação. O operador não viu a aceleração da rotação nas ultracentrífugas porque ele estava recebendo a informação de uma tela que havia sido gravada tempos atrás, com a informação que a operação estava normal e, dessa

forma, nenhuma providência foi tomada e outras ultracentrífugas continuaram acelerando até que se desintegraram.

O terceiro tipo de ataque é o *Denial of Control*: consiste na negação de controle. É quando o operador tem inibido o seu acesso e controle no sistema. Por mais que o alarme indique e sinalize que algo está acontecendo, ele não consegue intervir e fazer a operação que ele deveria fazer. O quarto tipo de ataque é a *Manipulation of Control*: consiste na manipulação de controle. É quando o comando que está sendo feito pelo operador é modificado sem que o operador perceba o que está sendo feito. O quinto tipo de ataque é o *Loss of Control*: consiste na perda de controle. É quando se tem a perda generalizada do controle da planta.

Esse tipo de informação está disponível nos mais diversos postos de vendas. Hoje em dia, há publicações disponíveis na *internet* e livrarias *online* que ensinam de alguma forma, a fazer ataques como esses (os cinco enunciados anteriormente).

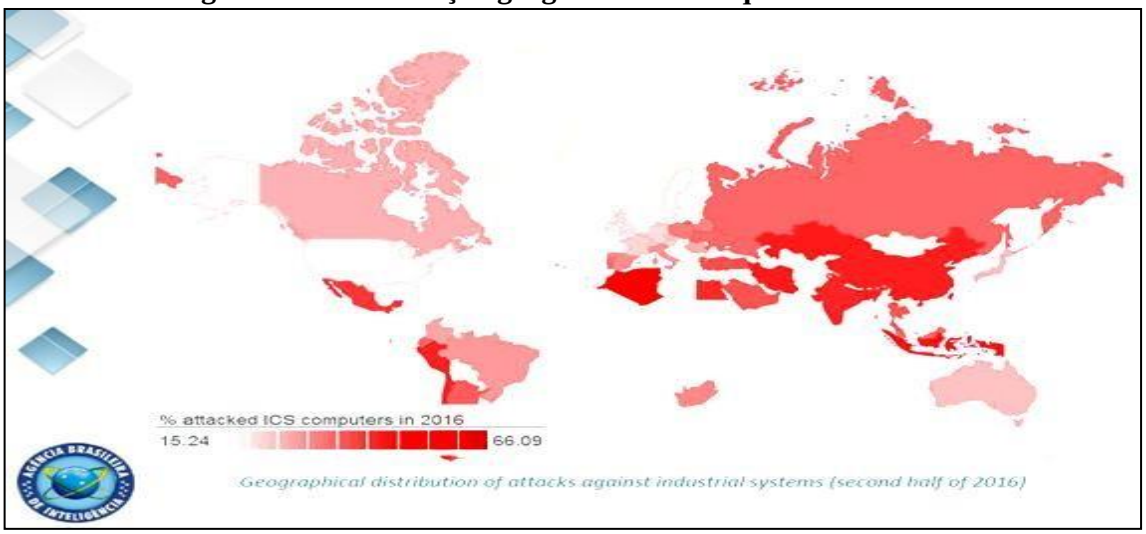
Figura 12 - Vulnerabilidades



Fonte: o autor, 2019.

O laboratório *Kaspersky* mapeou algumas vulnerabilidades em 2016 e constatou que em 45% dos ataques de negação de serviço, foram direcionados aos sistemas DOS. Houve ataques também em RCE, injections, manipulação de arquivos, manipulação de contas. Quando se analisa a incidência geográfica dos ataques, notam-se algumas surpresas como o Vietnã, que aparece em primeiro, seguido da Argélia. Na América do Sul, Peru e o Chile são grandes alvos de ataques e o Brasil não está entre os 15 principais destinos de ataques cibernéticos.

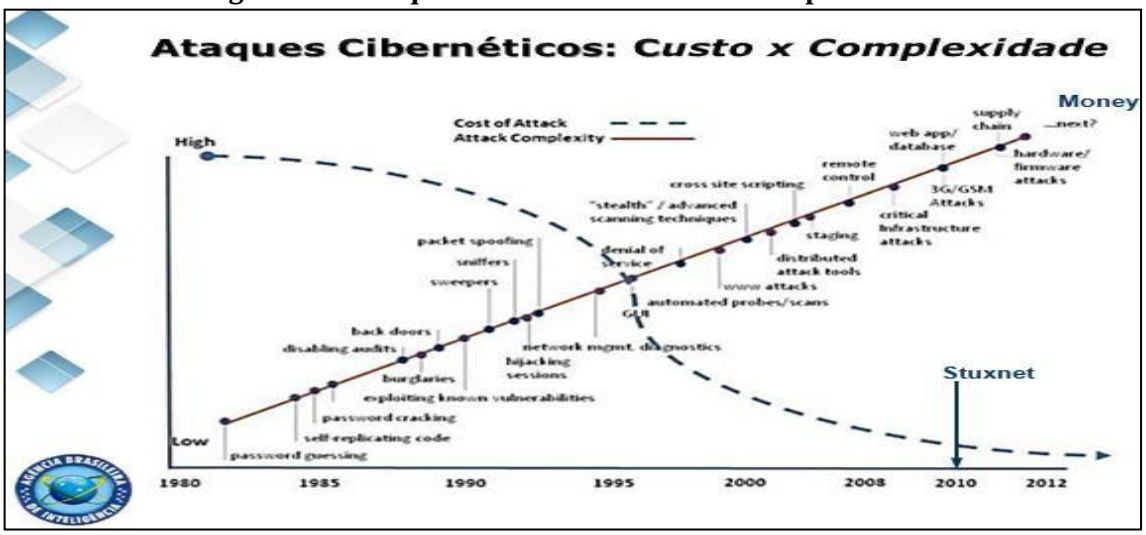
Figura 13 - Distribuição geográfica dos ataques cibernéticos



Fonte: o autor, 2019.

As principais fontes de ameaça são a *internet*, a mídia removível e os *emails*. Esse gráfico mostra uma tendência aparente sobre a questão do custo dos ataques e a complexidade dos mesmos:

Figura 14 - Ataques cibernéticos: custo X complexidade



Fonte: o autor, 2019.

Com o tempo, o custo dos ataques foi decaindo e a complexidade dos ataques foi aumentando. Isso se justifica pela disponibilidade de códigos e do tipo de conhecimento necessário para atingir os equipamentos. Esse *worm* atingiu pontos bastante específicos, pelo que se conclui que isso não foi coisa de pessoal de fundo de garagem, pelo contrário, boa parte dos ataques deve ter sido feito por um Estado.

Em 2010, não tinham como adivinhar a relevância do que havia caído na mesa deles, estavam apenas curiosos porque o *Stuxnet* continha algo raro que explorava o dia. Sempre que o *Stuxnet* infectava um novo computador, começava o trabalho para se descobrir o porquê de tais ataques. Quando encontrava o vírus, o mesmo já havia copiado

os CLPs por ter ficado um bom tempo na máquina (cerca de um mês). Eles perceberam que tinham encontrado algo de relevância mundial

Ao juntarem as pistas do código dos dados da Agência Internacional de Energia Atômica, eles conseguiram especificar uma determinada usina nuclear num local chamado *Natanz*. Quando a rede fosse infectada, o *Stuxnet* se desenrolaria da seguinte forma: ele tentaria dois mecanismos de ataque - um seria acelerar as centrífugas até 1410 Hz, o que faria com que os tubos de alumínio dentro das centrífugas vibrassem incontrolavelmente e quebrasse e - o outro seria reduzir a uma velocidade a 2 Hz. Em suma, enquanto as centrífugas girariam descontroladamente, o *Stuxnet* começaria a reproduzir os dados gravados quando tudo estava funcionando normalmente.

É como aqueles filmes que tem um funcionário de olho nas câmeras de vigilância e eles colocam uma sequência falsa. Dessa forma, os guardas de segurança não iriam perceber que o cofre estava sendo roubado naquele exato momento, que foi exatamente o que o *Stuxnet* fez. A diferença foi que o *Stuxnet* atuou no ambiente virtual do computador.

Mas o truque final viria quando os operadores tentassem fechar a usina, quando tentassem apertar o botão vermelho que enviaria um sinal para aqueles CLPs dizerem ao sistema parar de funcionar. Como *Stuxnet* infectou tais CLPs, o sinal foi cortado e permitiu que o ataque continuasse operando. E parece que funcionou, parece que o *Stuxnet* supostamente destruiu cerca de mil centrífugas, vindo a atrasar o programa nuclear do Irã em cerca de dois anos.

Mas há uma questão muito importante ainda em aberto: **Quem desenvolveu o *Stuxnet*?** Isso é coisa de gente grande. Infelizmente não temos nenhuma prova que nos diga que foi um país em particular. Ficou bem claro que estamos falando em nível de país e obviamente é algum que não é aliado do Irã e que está politicamente motivado para impedir o enriquecimento de urânio no Irã. Ninguém admitiu oficialmente estar por trás desse vírus, mas foi amplamente divulgado que o *Stuxnet* foi desenvolvido nos Estados Unidos da América com a ajuda de Israel, mas nenhum dos dois países assumiu a autoria da realização dos ataques.

O *Stuxnet* é um momento-chave da história da guerra cibernética. Antes, as pessoas sequer pensavam sobre a existência de armas cibernéticas de guerra, de programas maliciosos capazes de explodir tudo e o *Stuxnet* abriu essa porta e todos os países atualmente estão falando sobre ataque e defesa entre um país e outro com as armas cibernéticas de guerra. No mundo digital de hoje ninguém sabe direito quem está

invadindo quem, se são criminosos, adolescentes ou até governos.

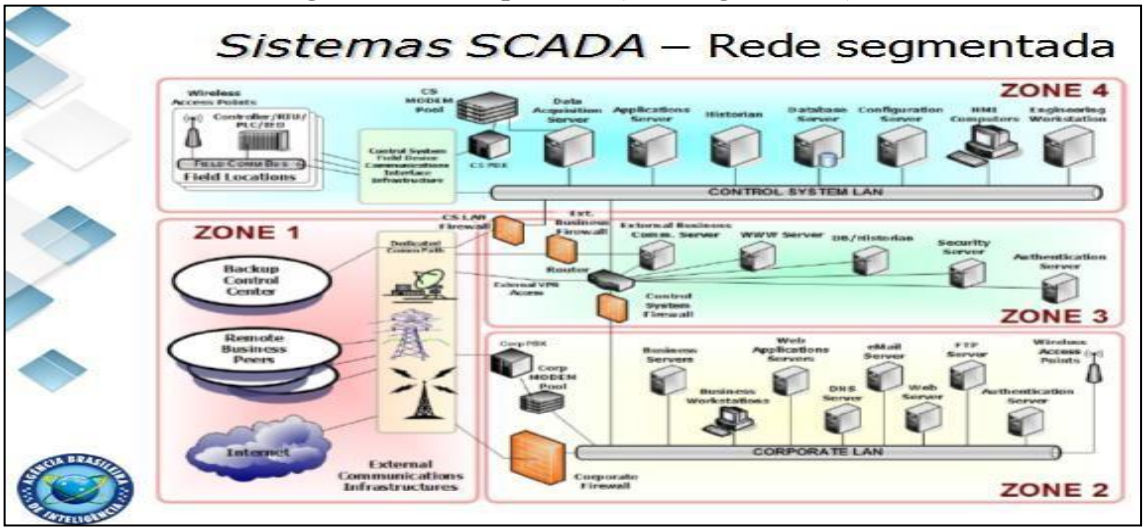
Em síntese, foi a primeira vez na história que chegamos a destruição física de equipamentos causada intencionalmente por um órgão que desenvolveu um vírus de computador. O *worn* pode estar circulando em diversos computadores, *pen drives* e dispositivos móveis. Não vão fazer absolutamente nada até serem conectados a uma rede de interesse, pelo que começarão a trabalhar e coletar informações com o servidor e poderão fazer de tudo.

3. Conclusões

Chega-se na parte final da apresentação com a certeza de que os ataques têm se tornado cada vez mais complexos e gerado menos custos. Algumas instituições, inclusive do governo, foram atacadas no estado do Rio de Janeiro. Já me deparei numa situação dessas e a principal preocupação das instituições residia na perda dos dados. Nosso conselho foi voltado na realização de ações preventivas, como um *backup* ou um *site* de contingência, que consiga restabelecer o funcionamento da rede da organização.

A proposta de solução para melhoria da segurança dos sistemas SCADA seria a segmentação da rede em zonas. A figura a seguir exemplifica essa questão:

Figura 15 - Boas práticas (rede segmentada)



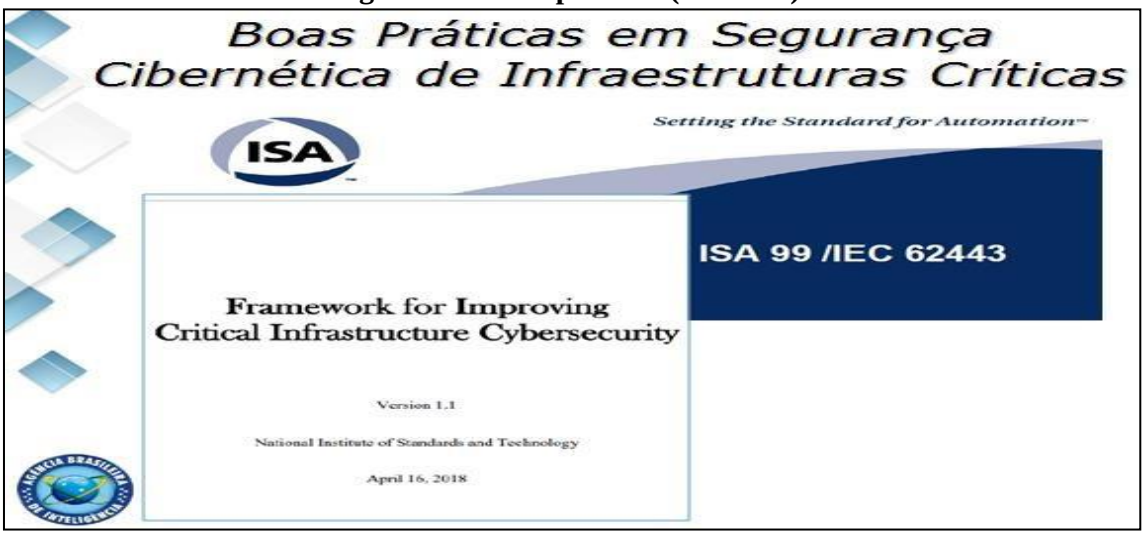
Fonte: o autor, 2019.

As zonas são separadas por *firewall*, sob uma forma um pouco mais inteligente: por IDSs. Essa segmentação é uma zona desmilitarizada que garante o fluxo das informações, bem como impede que um ataque consiga se propagar pela parte interna da rede e atinja os sistemas de controle e informação.

Como boas práticas, sugiro também a leitura do *framework* (NIST - série 800), que é documento que trata sobre a segurança cibernértica das estruturas críticas. Da

mesma forma, sugiro a leitura da norma ISA 99/IEC 62443, que dá as bases necessárias para realizar essas implementações:

Figura 16 - Boas práticas (manuais)



Fonte: o autor, 2019.

Obrigado e me perdoem pela demora!

POLÍTICAS PÚBLICAS DE DEFESA CIBERNÉTICA EM PERSPECTIVA COMPARADA: UMA ANÁLISE DOS CASOS DE EUA, CHINA, RÚSSIA E ISRAEL

Dannielle Jacon Ayres Pinto*

1. Introdução

Bom dia a todos.

É um prazer novamente estar aqui nessa casa, local onde faço meu pós-doutoramento. É uma oportunidade única poder falar para um público que, de alguma forma, pode ajudar na construção dos documentos de *ciberdefesa* do Brasil nos próximos anos.

A proposta desse encontro é compreender o caso de alguns países específicos, mais precisamente os Estados Unidos da América (EUA), China, Rússia e Israel. Busca-se verificar se os documentos de defesa desses países possuem ou falam algo relacionado à *ciberdefesa* e *cibersegurança.* Na sequência, procura-se estabelecer uma comparação entre os documentos de defesa, mais precisamente trazendo a reflexão de como a *ciberdefesa* e a *cibersegurança* estão sendo desenvolvidas no âmbito da Defesa.

Na academia, é frequente a tentativa de se definir os conceitos de *ciberdefesa* e de *cibersegurança*, mas sem dispensar as definições já existentes no sistema internacional sobre *ciberdefesa* e *cibersegurança.* Quando se observa os documentos de defesa, verifica-se realmente o que os Estados irão produzir em termos de *ciberdefesa* e *cibersegurança*, não pelo fato de conter conceitos melhores, mas tão somente por discriminar as ações que serão realizadas pelos Estados na ordem internacional.

Dessa feita, por mais que se possa academicamente contestar os conceitos contidos, é uma tarefa árdua fazer com que os conceitos acadêmicos sejam mudados pelos Estados. De um lado, a tendência é que os documentos determinem como o Estado se organiza e de outro lado, a tendência é que a academia vai determinar alguns conceitos de países centrais, os quais venham a se tornar em modelos para Estados como o Brasil.

Diante do exposto, espera-se que os documentos de defesa desses países (EUA, China, Rússia e Israel) possam se constituir numa matriz base para a elaboração de

* Estagiária de Pós-Doutorado em Ciências Militares, na Escola de Comando e Estado-Maior do Exército.

documentos de defesa para países como Brasil. Não tem como escapar de uma pré-influência de uma série de conceitos que se estudam nos países centrais nessa área.

2. Desenvolvimento

A primeira pergunta que se faz é a seguinte: Por que foram selecionados a China, Rússia, Israel e Estados Unidos? Se pesquisar alguns índices de segurança cibernética ou de defesa cibernética, vai perceber que esses quatro países não estão entre os dez países mais seguros na cibernética, de acordo com o *ranking National Cyber Security Index*, produzido na Estônia. Nesse *site*, podem ser verificados os países que estão mais preparados para evitar um ataque cibernético e os que estão mais aptos para responder a este ataque, conforme demonstra a figura a seguir:

Figura 1 - *Ranking National Cyber Security Index*

Rank	Country	National Cyber Security Index	Digital Development Level	Difference
1.	Czech Republic	90.91	69.37	21.54
2.	Estonia	90.91	79.27	11.64
3.	Spain	89.61	73.24	16.37
4.	Lithuania	88.31	70.95	17.36
5.	Greece	87.01	65.44	21.57
6.	France	83.12	79.06	4.06
7.	Finland	81.82	82.26	-0.44
8.	Denmark	81.82	83.55	-1.73
9.	Netherlands	81.82	83.88	-2.06
10.	Germany	80.52	81.95	-1.43

Fonte: o autor, 2019.

Consideração importante deve ser feita para Alemanha e França, países grandes em termos populacionais e que estão entre os 10 mais seguros em cibernética. Os demais países contam com uma população pequena, mas com capacidade de segurança muito grande.

Se buscarmos o posicionamento de Israel, Rússia, EUA e China, verificaremos que os mesmos estão em posições intermediárias, com a Rússia ligeiramente melhor do que Israel e os EUA. A China, efetivamente, é a que ocupa uma posição mais baixa nesse *ranking*. Esse dado nos leva ao entendimento de que esses quatro países não são tão seguros sob o ponto de vista da segurança cibernética ou da defesa cibernética:

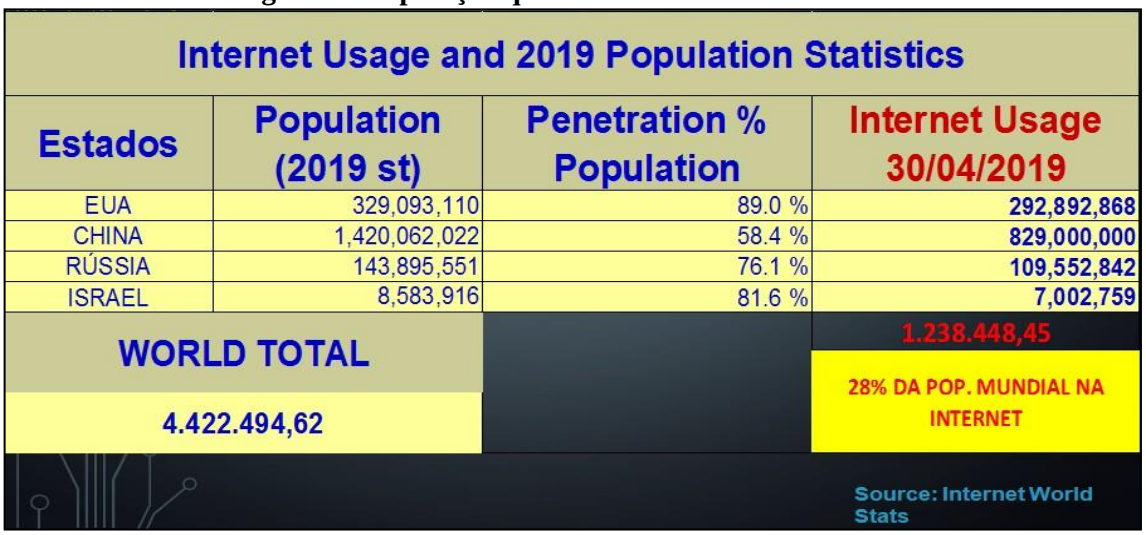
Figura 2 - *Ranking National Cyber Security Index* (EUA, Rússia, China e Israel)

Fonte: o autor, 2019.

Não existe uma metodologia específica. O *site* peca na explicação da metodologia utilizada para estabelecer o *ranking*, pelo que não dá a robustez e a confiabilidade necessária aos dados apresentados. Porém, é muito interessante ver que países como a Estônia, que possui uma compreensão singular acerca do tema em pauta, melhor posicionada que os Estados centrais, supostamente em defasagem e num nível de desenvolvimento mais baixo nesse tema.

No entanto, EUA, Israel, China e Rússia são atores importantes nesse tema porque são países que, efetivamente, controlam a agenda internacional de defesa, determinando o que deve ou não ser estudado. Um dado importante é que esses países em conjunto são responsáveis por 28% da população mundial que acessa a *internet*:

Figura 3 - População que utiliza a *internet* no mundo



Fonte: o autor, 2019.

A China, por seu turno, mesmo contando com a maior população atrelada a *internet*, só tem 58% de penetração da *internet* entre os seus cidadãos, fato que induz ao

questionamento se os chineses são falhos ou estão deixando de perceber algo ou se eles efetivamente estão construindo uma estratégia cibernética com ideia abstrata. Israel foi selecionado por ser o mais desenvolvido do mundo, sob o ponto de vista dos recursos cibernéticos e dos recursos cibernéticos militares.

Para que eu possa falar que a guerra cibernética é X e que a guerra cibernética em outro momento é Y. Que um terrorista cibernético é A e em outro momento é B, esses termos precisam estar bem definidos nos principais documentos de defesa. Esses documentos, infelizmente, não fogem da lógica do poder que cada país exerce no globo. O primeiro caso são os EUA, país que tem supostamente mais documentos que legislam sobre *ciberdefesa*, *cibersegurança,* conceito de guerra cibernética e outros. Esses documentos são os principais confeccionados desde 2016:

Figura 4 - Legislação nos EUA

País	Principais Documentos de Defesa Cibernética	Ano	Orgão promotor
EUA	Summary of Objectives for the NAFTA Renegotiation	2017	Office of the US Trade Representative (USTR)
	National Security Strategy of the United States of America	2017	White House
	National Cyber Strategy of the United States of America	2018	White House
	Cybersecurity Strategy	2018	US Department of Homeland Security (DHS)
	National Intelligence Strategy	2019	Office the Director National Itelligence (DNI)
	National Defense Strategy	2019	Department of Defense (DoD)

Fonte: o autor, 2019.

O fato interessante no modelo norte-americano é que ele já começa a pensar juntamente com a China. Esses documentos já falam alguma coisa sobre a inclusão e o controle que o Estado pode ter junto ao setor privado, que se atacados terão consequências no poder público. Nesse sentido, os EUA já começam a pensar na relação estabelecida entre o poder público e o setor privado. Quando os EUA pensaram em defesa cibernética e em segurança cibernética, eles abriram um caminho que atende o setor privado e outro que atende os interesses públicos (soberania e defesa).

Nesse primeiro documento (*Summary os Objectives for the NAFTA Renegotiation*), elaborado em 2017, nota-se que os EUA já trabalham com a idéia de que o comércio digital e as consequências advindas dessa prática são elementos centrais na idéia da defesa cibernética do Estado norte-americano, pelo que se conclui que o governo norte-americano trata dessa questão como sendo uma área de interesse nacional. Nos

outros documentos, constata-se que a elaboração desse tipo de documento normalmente fica sob o encargo do escritório de comércio dos EUA.

Entrementes, já começa a expandir a percepção do que é ou não importante nas questões afetas a cibernética. Em outros documentos como a *National Security Strategy of the USA* - 2017 e a *National Cyber Strategy of the USA* - 2017, percebe-se que os EUA conseguem definir bem os conceitos cibernéticos e as propostas de defesa e segurança cibernética. Cumpre destacar que os mesmos pensam a *ciberdefesa* e a *cibersegurança* na camada estratégica e na camada política.

O *Cyber Security Strategy - 2018*, a *National Inteligence Strategy - 2019* e a *National Defense Strategy - 2019* ensinam a utilizar de maneira ofensiva a cibernética, e por isso são estratégicos, políticos, operacionais e táticos.

O *National Defense Strategy*, feito pelo Departamento de Defesa dos EUA, versa sobre as dimensões do domínio da guerra. O *ciberespaço* é considerado como sendo um domínio na doutrina norte-americana, mais precisamente um espaço onde se exerce poder e que pode ter uma Força Armada mobiliando esse espaço. A China e a Rússia já possuem até a quinta Força Armada (setor espacial e setor cibernético).

Os EUA caminham para isso, porque eles compreendem que os computadores são armas, e dessa forma, podem carregar vírus. Já existe um setor só dedicado ao *site space*. Ou seja, os norte-americanos partem do pressuposto que podem ser deflagradas guerras no espaço virtual. Se eu posso utilizar um tanque no terreno, se eu posso utilizar um navio no mar, por que eu não posso utilizar o computador como uma arma? Se é uma arma, todos podem ter o acesso e uma série de dilemas podem ser colocados à tona.

O segundo país é a China. Ela tem menos documentos que os EUA, mas os documentos chineses tem uma particularidade interessante, qual seja: os documentos chineses já começam a criar o alicerce para que o país influencie no sistema internacional a partir da sua compreensão, da sua demanda e sobre o que os chineses entendem serem responsáveis sobre segurança e defesa. A percepção chinesa desse tema abarca também a área privada, com todos os óbices possíveis. Os documentos de defesa na China abordam a área privada com o intuito de evitar que esse setor crie um problema, caso não se proteja. Os pricnipais documentos são os seguintes:

Figura 5 - Legislação na China

País	Principais Documentos de Defesa Cibernética	Ano	Orgão promotor
CHINA	National Cyberspace Security Strategy	2016	CAC - Cyberspace Administration of China
	Cybersecurity Law of the People's Republic of China	Promulgada em 2016 3 implementada em 2017	Standing Committee of the National People's Congress
	International Strategy of Cooperation on Cyberspace	jul/05	Ministery of Foreign Affairs
	White Book - China's National Defense in The New Era	2019 (Julho)	The State Council Information Office of the People's Republic of China

Fonte: o autor, 2019.

A China tem um documento de 2016, feito pelo CAC, que é o *National Cyberspace Security Strategy*, que começa a tratar sobre uma Estratégia Nacional de *cibersegurança* da China. Este documento traz alguns elementos interessantes. Todavia, o documento mais interessante da China é o *Cybersecurity Law of the People's Republic of China*, o qual obriga as empresas de tecnologia na China a serem submetidas por processos de segurança rotineiros por parte do Estado, além de tornar obrigatório o armazenamento de todos os dados dos seus usuários para que o governo chinês utilize em caso de crime cibernético, em caso de problemas na área cibernética. Ou seja, é o primeiro documento estatal onde é possível ver um país impondo restrições, limites e obrigações ao setor privado com relação às conseqüências dos ataques cibernéticos. A China hoje é um expoente e pode servir de modelo no futuro, mesmo que seja o modelo repensado por nações ocidentais.

Outro documento muito interessante é o novo Livro Branco de Defesa da China, que foi publicado em 19 de julho de 2019. O mesmo traz muitas coisas interessantes. No que concerne a *cibersegurança* e *ciberdefesa*, um aspecto interessante reside na explicação de como estão sendo desenvolvidas as capacidades de *cibersegurança* nos meios de defesa, o que os tornam mais consistentes quando comparados aos padrões internacionais, conferindo o *status* de ser o maior país cibernético do mundo. Na verdade, entende-se que isso é um problema, pois um país como a China, que segue padrões distintos em relação a ordem política e social, quando começa a exercer alguns tipos de liderança no sistema internacional, algo pode ser reestruturado.

O próximo país é a Rússia, que tem uma quantidade interessante de documentos, mas que tem uma peculiaridade: todos os documentos de defesa são decretos e na sua maioria, não chegam a virar lei, conforme a figura abaixo:

Figura 6 - Legislação na Rússia

País	Principais Documentos de Defesa Cibernética	Ano	Orgão promotor
RÚSSIA	Decreto N31C	2013	President of the Russian Federation
	Doutrina de Segurança de Informação da Federação Russa	2016	President of the Russian Federation
	Lei N-187-FZ (Sobre a segurança da infra-estrutura de informações críticas da Federação Russa)	2017	President of the Russian Federation
	Decreto N-620	2018 (elaborada em Dezembro de 2017)	President of the Russian Federation
	Estratégia para o Desenvolvimento da Sociedade da Informação na Federação Russa para 2017-2030	2017	President of the Russian Federation

Fonte: o autor, 2019.

Apesar da Rússia se considerar uma das mais capazes na resposta aos ataques cibernéticos, não temos noção do que eles pensam sobre *ciberdefesa* e *cibersegurança*. Isso se deve pelo fato de que os documentos são submetidos ao presidente e ele está politicamente submetido à vontade a demanda da Rússia. Os documentos russos possuem o viés político muito forte e por questões de idioma, torna-se difícil realizar uma análise sobre o teor dos mesmos.

O último país a ser analisado é Israel, que também tem pouquíssimos documentos conforme apresentado na figura a seguir:

Figura 7 - Legislação em Israel

País	Principais Documentos de Defesa Cibernética	Ano	Orgão promotor
ISRAEL	Resolução 2443 e 2444	2015	Government of Israel
	Israel Defense Forces (IDF) Strategy	2015	IDF, que agora é Office of National Cyber Directorate
	NATIONAL CYBER CONCEPT FOR CRISIS PREPAREDNESS AND MANAGEMENT	2018	Prime Minister-s office National Cyber Directorate

Fonte: o autor, 2019.

Israel não tem nenhum documento traduzido para o inglês. O governo israelene não traduz seus documentos porque os mesmos são extremamente estratégicos e relacionam-se com a defesa da soberania do Estado. Ter os conceitos cibernéticos escritos e publicados somente para aqueles que falam hebraico, quer dizer que o documento é direcionado somente para o seu público de interesse. De toda sorte, constatou-se que o *National Cyber Concept for Crisis Preparedness and Management* foi o único documento de defesa cibernética israelense que foi traduzido. Trata-se de uma tradução feita pela Universidade de *Harvard* para o idioma inglês, pelo que possibilitou a extração de algum tipo de informação. Um aspecto interessante é a organização que o Estado de Israel promove sobre o tema na esfera nacional e na esfera da sociedade civil. Em linhas gerais, nota-se que os documentos de defesa cibernética israelense trazem definições somente sob o ponto de vista de Israel e se constituem numa estratégia de defesa.

Se pensarmos que o espaço cibernético tem três camadas: *hardware, software* e aquilo que o pessoal costumeiramente chama de *people*. Quando se olha efetivamente para o recurso central do *ciberespaço,* que é a *internet,* nota-se que as pessoas também são centrais. Dessa forma, não há elementos de como tratar esse espaço tão rapidamente.

Uma pesquisa feita em 2019 apontou a tendência da utilização das mídias sociais no planeta. Em 2010, havia menos de um bilhão de pessoas utilizando a *internet* e em 2021 a pesquisa apontou que cerca de três bilhões de pessoas estarão utilizando a *internet*. Ou seja, algo em torno de 45% a 47% da população mundial estarão nas mídias sociais em 2021, pelo que vai tornar o sistema mais vulnerável ainda, uma vez que mais pessoas estarão utilizando a *internet*.

Em 2009, 0,7% do acesso feito à *internet* era por aparelho celular e em 2018, a pesquisa apontou que 52.2% da população acessavam a *internet* por meio de equipamentos celulares, aspecto central e talvez o de maior vulnerabilidade atual quando se fala em documento de Defesa.

O volume financeiro que circulou no comércio mundial em 2016 por meio de equipamento celulares foi em torno de 970 bilhões de dólares, representando algo em torno de 52,4% do comércio mundial no mesmo ano. Em 2021, estima-se que 72,9% do comércio mundial será feito por meio dos telefones celulares, o que representará um montante na ordem de 3 trilhões e 560 bilhões de dólares.

3. Conclusões

E como essa equação é resolvida? Eu acho que não tem outra solução e no meu entendimento, o aspecto central é a mudança de atitude. Todas as pessoas precisam entender sobre segurança e defesa cibernética. Se o setor privado não tiver capacidade de pensar a segurança cibernética como um fruto que gera inovação e economia, então é necessário pensar na elaboração de documentos que estejam alinhados com a tripla hélice:

Figura 8 - Uma estratégia em comum

Fonte: o autor, 2019.

Por fim, entendo que os documentos de defesa cibernética e de segurança cibernética elaborados nesses países (EUA, Rússia, China e Israel) são importantes porque os mesmos podem servir de base para a elaboração dos documentos de defesa que estejam alinhados e adequados segundo a realidade do Brasil.

Muito obrigado pela atenção!

CIBERSEGURANÇA OU *CIBERDEFESA*? CONCEITOS E EXPERIÊNCIAS EM PAÍSES DIFERENTES

Daniel Oppermann*

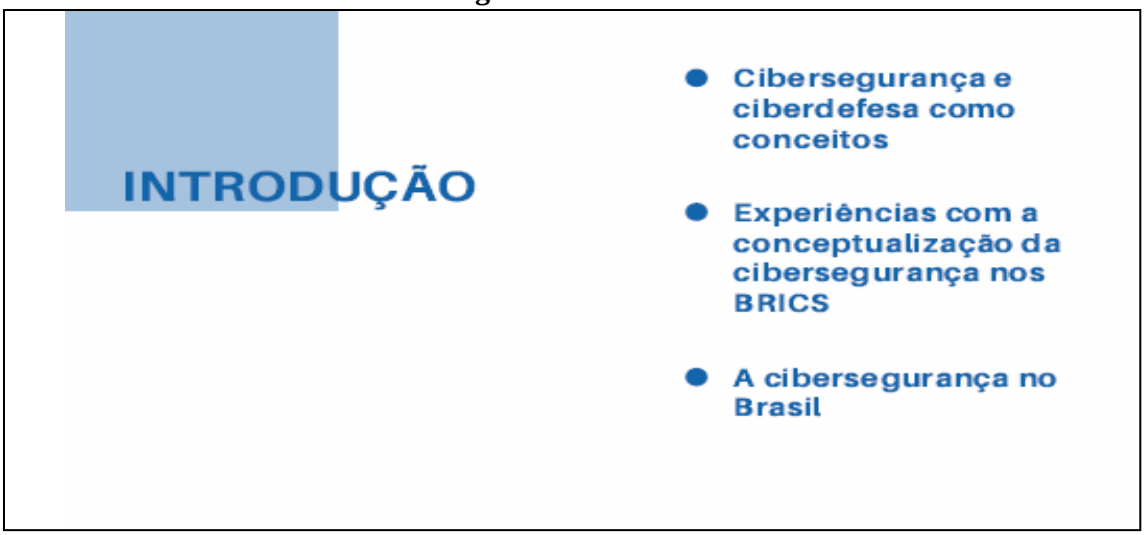
1. Introdução

Bom dia.

Agradeço a presença de todos nesta sala. Sou cientista político com foco em relações internacionais, segurança cibernética e governança da *internet*. Faço pós-doutorado conduzido pela Escola de Comando e Estado-Maior do Exército sobre defesa cibernética e procuro analisar o discurso da academia sobre defesa cibernética e segurança cibernética no Brasil.

O título já é o foco da minha apresentação sobre *cibersegurança*, haja vista que não é *cibersegurança* em si, mas sim um *ciber* para a defesa também, porque a gente não sabe ainda o que realmente é *cibersegurança* e o que realmente é *ciberdefesa*. Utlizam-se muitos conceitos, mas por enquanto não há definições próprias, não existem conceitos bem desenvolvidos na academia. Esse é o foco da minha apresentação: falar sobre as experiências em países diferentes, com ênfase nos BRICS e se sobrar tempo, posso falar depois um pouco sobre a Alemanha. A apresentação terá o seguinte sumário: a primeira abarcará a questão conceitual que envolve a segurança cibernética. Depois serão tratadas as experiências acerca da conceitualização de *cibersegurança* nos BRICS e na parte final a segurança no Brasil, conforme especificado a seguir:

Figura 1 - Roteiro



* Doutor em Relações internacionais e Estagiário de Pós-Doutorado em Ciências Militares, na Escola de Comando e Estado-Maior do Exército.

Fonte: o autor, 2019.

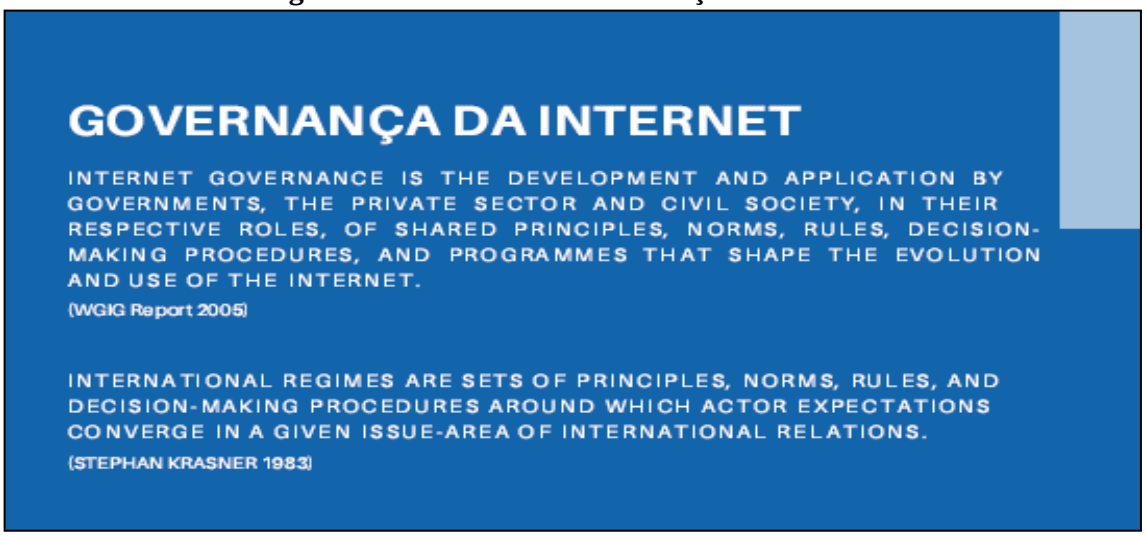
2. Desenvolvimento

A *cibersegurança* e a *ciberdefesa* é a base da pesquisa que desenvolvo com a ECEME. Uma pesquisa sempre começa com certas definições conceituais, as quais servem para enriquecer o debate e para definir especificamente qual conceito será utlizado no transcorrer da pesquisar. Os conceitos são essenciais para as pesquisas acadêmicas. Como o ambiente *ciber* é composto por várias áreas diferentes, vou focar os conceitos na área que envolve as relações internacionais e a ciência política. Eu trabalhava com o pessoal da área jurídica e temos colegas das áreas de engenharia, todo mundo trabalha com conceitos, mas todo mundo aborda os conceitos de outra forma.

Quando olhamos os conceitos, percebemos que eles vêm de várias áreas do conhecimento, entretanto nenhuma delas foi capaz de elaborar um bom conceito. Como a *cibersegurança* é um tema novo, percebe-se que a mesma ainda não tem uma própria definição. Na verdade, na academia esses conceitos são discutidos por muitos anos.

Eu vou trazer alguns exemplos dos últimos anos: o conceito de governança da *internet* foi desenvolvido em 2005 e publicado no mesmo ano num periódico. O grupo desenvolveu uma definição do conceito de governança da *internet*, pela primeira vez na época. Todavia, alguém já percebeu a origem dessa definição? Essa definição foi desenvolvida pelos anos 1980. Em vista disso, percebe-se que a definição de 2005 foi altamente influenciada pela definição do estilo clássico dos anos 1980:

Figura 2 - Conceito de Governança da *Internet*



Fonte: o autor, 2019.

E verificamos esse aspecto em vários conceitos também. Outro exemplo é o conceito de segurança cibernética contido na Doutrina Militar de Defesa Cibernética do Brasil - 2014: Segurança cibernética é a arte de assegurar a existência e a continuidade da

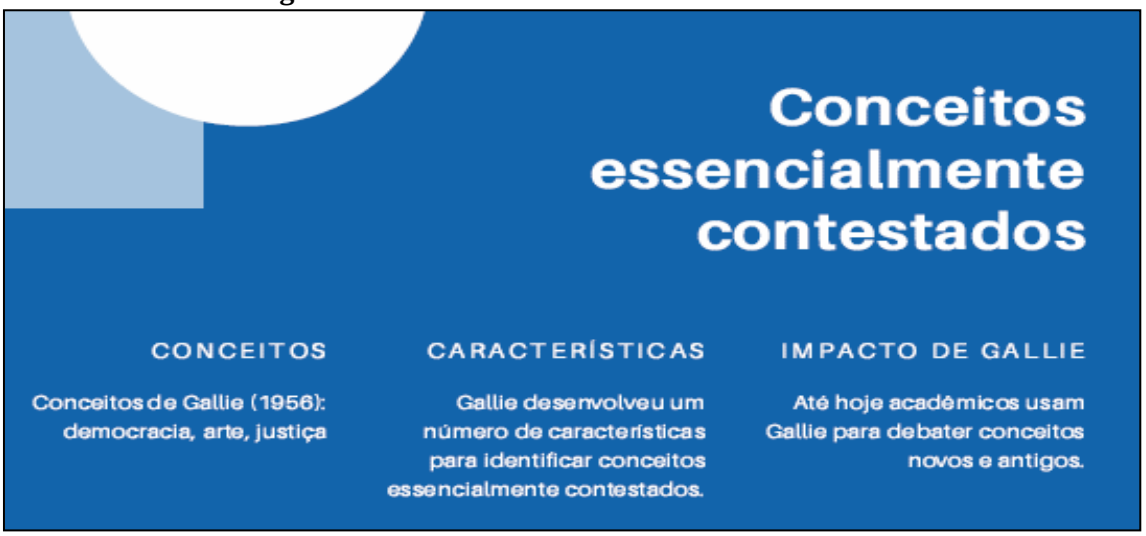
sociedade de informação de uma nação, garantindo e protegendo no espaço cibernético os ativos de informação e suas infraestruturas críticas. Essa definição é sob o contexto do regime militar de defesa cibernética. Existe também a lei geral de proteção de dados, que foi elaborada no ano passado possui a definição de vários conceitos:

Figura 3 - Conceitos contidos na Lei geral de Proteção de dados

Fonte: o autor, 2019.

Em 1956, o cientista político da Grã Bretanha *Walter Bryce Gallie* publicou um *paper* que dizia que conceitos contestados eram capazes de gerar grande influência no desenvolvimento de outros conceitos e que ainda hoje influenciam inclusive na área de segurança cibernética. Esse *paper* apresenta a dificuldade de se definir conceitos de forma completa. Em suma, ele está discutindo conceitos que são tão amplos, mas que várias pessoas têm suas próprias abordagens e suas teorias sobre isso.

Figura 4 - Conceitos essencialmente contestados



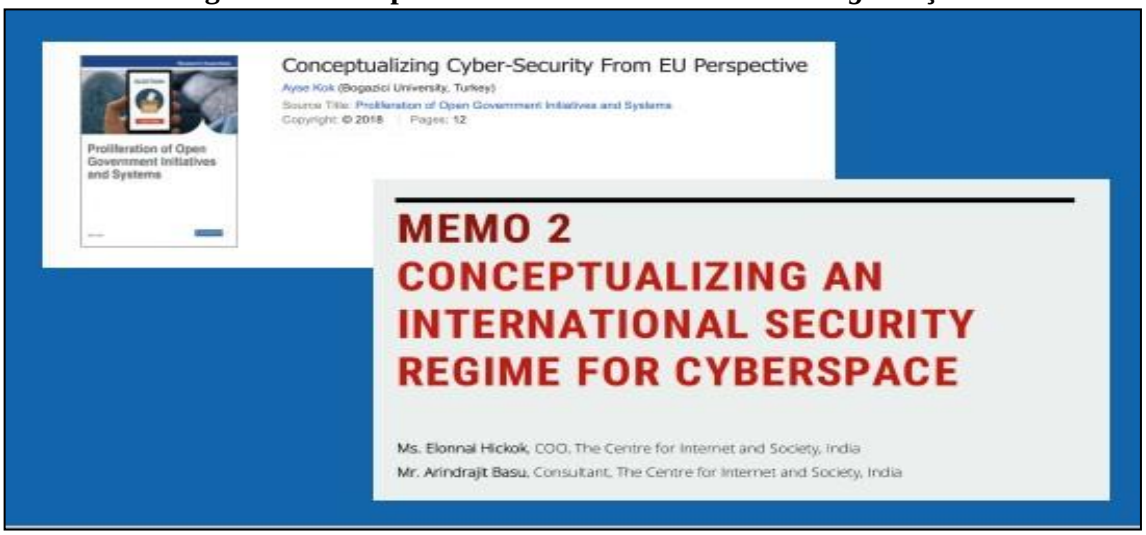
Fonte: o autor, 2019.

Ele desenvolveu um número de características para identificar os conceitos essencialmente contestados. Ou seja, conceitos que são amplamente discutidos e que tem várias definições, mas que foram desenvolvidas por pessoas diferentes. Isso é um grande desafio. Como deve ser o debate sobre a segurança cibernética? Por que existem conceitos que são amplamente diferentes de segurança cibernética? São por essas questões que o desenvolvimento de conceitos é tão essencial na academia.

Até hoje, inclusive na questão de segurança internacional, usa-se bastante essa probabilidade de ação, que é frequentemente apresentada nos debates acadêmicos sobre conceitos de segurança. O primeiro começou com o conceito de segurança. Se por um lado, observa-se na literatura que há um amplo debate sobre a questão de segurança. Por outro lado, verifica-se que o conceito de segurança não é amplamente definido.

No que concerne a *cibersegurança*, nota-se que a mesma é um tópico tão novo que não se pode esperar uma definição pronta ou um conceito já bem desenvolvido. Dessa forma, constata-se que ainda falta um debate conceitual sobre *cibersegurança*, *ciberdefesa*, *ciberguerra*, *ciberarmas*, etc. Em síntese, não tem debate ainda sobre o que realmente é uma *ciberarma* ou o que significa *ciberdefesa.*

Figura 5 - Exemplos de conceitos relativos à *cibersegurança*



Fonte: o autor, 2019.

Esses dois exemplos são de pessoas que tentaram nos últimos anos iniciar conceptualizar *cibersegurança*. Uma pessoa é oriunda de uma Universidade na Turquia. E tem o conceito de segurança que foi desenvolvido por colegas do *Center for Internet Society*, da Índia, e que foi publicado num grupo de pesquisa europeu. Ou seja, verifica-se que existem poucas contribuições da academia sobre o conceito de *cibersegurança*.

Com essa realidade, torna-se imperioso que a academia possa contribuir para o desenvolvimento do conceito de *cibersegurança*. Houve uma tentativa nos últimos meses,

no âmbito do projeto dos BRICS, onde estava a FGV - Escola de Direito. O projeto dos BRICS é um projeto de análise de políticas digitais implementadas nos países pertencentes aos BRICS e nesse sentido, o conceito de *cibersegurança* foi trabalhado e desenvolvido na Escola de Direito, mas somente isso é incipiente. Cada Escola forma o pensamento. Todo mundo tem suas próprias abordagens. Essa foi uma tentativa com base no pensamento jurídico. Dessa forma, o conceito de *cibersegurança* foi inserido como sendo o conceito principal e dentro dele foram colocadas outras cinco definições. Isso faz sentido na análise jurídica, especialmente para os BRICS.

Na sequência, será apresentado como a *cibersegurança* está categorizada: *cibercrime*, *ciberdefesa*, proteção de dados, ordem pública e proteção do consumidor.

Figura 6 - Categorização da *cibersegurança*

Fonte: o autor, 2019.

No âmbito dos BRICS, a China é o único país em que a ordem pública conversa com o setor privado a respeito de segurança cibernética. Os chineses possuem uma conscientização sobre a proteção do consumidor e uma abordagem jurídica desenvolvida acerca do tema, até porque o consumo *online* é bastante expressivo na China. Nessa perspectiva, a *cibersegurança*, sob o ponto de vista do usuário, inclui também a produção do consumidor.

Essa é uma abordagem dedutiva, ou seja, pegam-se algumas idéias e desenvolvem-se os conceitos baseados nas mesmas. A idéia principal se baseou em quais leis precisavam ser analisadas. Quais conceitos precisavam ser inseridos em nosso contexto. Se fosse uma abordagem indutiva, teríamos primeiramente que analisar o campo, os dados e depois desenvolver os conceitos. Isso é uma grande diferença. Por exemplo, na área jurídica tem muito trabalho dedutivo, porque muitas coisas já são pré-definidas. Já na área das ciências sociais, da ciência política, das relações internacionais

e das ciências militares, primeiro os dados são coletados, depois os mesmos são analisados e só depois dessas ações é que se chega a uma conclusão. E daí pode sair um conceito de *cibersegurança* no Brasil.

Qual nível de desenvolvimento está a *cibersegurança* no Brasil? Para obter essa resposta, foram analisadas várias leis, inclusive a questão de *cibercrime* e proteção de dados. A questão decisiva é que o crime no Brasil é definido por um conjunto de leis. Dentre todas elas, a principal é a lei de crime cibernético, que trata sobre a invasão de dispositivos e vazamentos de dados, promulgada em 2012.

Geralmente quando as leis são bem desenvolvidas, as mesmas trazem consigo vários conceitos e definições. Para que se tenha uma ideia do nível de desenvolvimento da lei que trata sobre *cibercrimes*, constata-se que a mesma quase não tem conceitos e definições, pelo que a torna bastante incipiente e curta. Nestes termos, conclui-se que a questão de crime cibernético é pouco definida no Brasil. Por outro lado, verificou-se a existência de outras leis que, quando juntadas, conseguem mostrar um cenário, mas não passa disso. Ou seja, não há uma lei com conceitos amplamente definidos.

Figura 7 - A *cibersegurança* no Brasil

Fonte: o autor, 2019.

Todavia, verifica-se que a lei geral de proteção de dados é uma lei bem desenvolvida, mesmo sendo baseada em outras leis. Essa lei foi promulgada em 2018 e fala principalmente do tratamento de dados, da segurança de dados, quem pode acessar quais dados, quais são os direitos do usuário, etc. Ou seja, a lei geral de proteção de dados busca trazer seriedade na relação estabelecida entre o setor privado, o setor público e as pessoas em geral. Existem algumas regulações específicas e exceções para a Defesa Nacional e para a Segurança Pública.

Quando esse tema é analisado sob a ótica da Defesa nos países pertencentes aos BRICS, nota-se que existe tem uma ampla quantidade de documentos que foram desenvolvidos nos últimos anos. No caso do Brasil, verifica-se que o tema começou com a Estratégia Nacional de Defesa de 2008, onde pela primeira vez foi mencionado o seu espaço como área estratégica importante. Depois disso, outros documentos que fizeram menção ao *ciberespaço* foram lançados. Nesse rol de documentos, destaque a parte deve ser dado para a Doutrina Militar de Defesa Cibernética, elaborada em 2014, a qual trouxe algumas informações e conceitos importantes. No que concerne aos conceitos, percebe-se que os mesmos foram definidos de forma bem curta e com vários níveis de abordagens diferentes. Ou seja, a Doutrina Militar de Defesa Cibernética é um documento essencial para a Defesa e para a *ciberdefesa* no Brasil.

3. Conclusões

Como conclusão, entendo que os desafios que o Brasil possui nessa área são válidos para os demais Estados, porque todos estão numa situação parecida. Quando se observa o que é comentado e falado em outros países, verifica-se que falam sempre a mesma coisa. Eu assisti um debate sobre o tema num determinado país e passaram-se alguns dias, assisti outro debate em outro país e para a minha surpresa, o assunto era o mesmo: a necessidade de se obter mão de obra qualificada, de investimento, de treinamento e de preparação dos usuários da *internet*. Essas necessidades são comuns a todos os países, e não é somente uma exclusividade do Brasil.

Então a questão é: Como avançarmos nesse tema se o país necessita de mão de obra qualificada? Tudo paira sobre a questão educacional, ou seja, o aspecto central desse tabuleiro estratégico reside em como desenvolver a segurança cibernética no ensino superior do país.

Por isso que é sempre importante a realização de um debate público sobre a segurança e defesa, pois ajuda no desenvolvimento de nossos conceitos com os usuários gerais. A população em geral não sabe como se comportar *online* pra diminuir certos riscos que as mesmas estão correndo. Sabe-se que ataques cibernéticos, muitas das vezes, são originários de computadores de usuários gerais. E eles precisam ter essas informações, pois precisam ser informados sobre o que está acontecendo no *ciberespaço* e o que eles devem fazer para se proteger e proteger a rede inteira.

Quero agradecer sua atenção destinada até agora.

Muito obrigado!

POLÍTICAS PÚBLICAS DE DEFESA CIBERNÉTICA EM PERSPECTIVA COMPARADA - REPÚBLICA ARGENTINA

Major Mariano Oscar Gómez (Exército da Argentina)*

1. Introdução

Bom dia.

É uma grande satisfação estar na Escola de Comando e Estado-Maior do Exército para falar sobre o meu país: a Argentina. A proposta é comentar sobre as políticas públicas de segurança e defesa cibernéticas adotadas pela Argentina, da mesma forma que vou estabelecer uma comparação entre a política pública de segurança e defesa cibernética adotada na Argentina e a congênere utilizada no Brasil, pontuando os aspectos que são diferentes.

A *ciberdefesa* argentina tem sua origem no Brasil, que foi o grande fornecedor de capacidades para que a concepção da atual estrutura cibernética da Argentina.

2. Desenvolvimento

Na Argentina, existem três níveis de condução cibernética: *ciberguerra* (segurança informática), *ciberdefesa* e *cibersegurança:*

Figura 1 - Níveis de condução cibernética na Argentina

Fonte: o autor, 2019.

* Oficial Instrutor de Nação Amiga (Argentina) junto à Escola de Comando e Estado-Maior do Exército.

A segurança informática compreende ao conjunto de medidas preventivas, de detenção e corretivas, vocacionadas a proteger a integridade, confidencialidade e disponibilidade dos recursos informatizados. Ou seja, são as ações realizadas no campo tático. A *cibersegurança* se refere à proteção das infraestruturas críticas diante das ameaças e agressões cibernéticas, proporcionando a tão desejada liberdade de ação para o emprego da infraestrutura, de acordo com os alinhamentos estabelecidos na Política de *Cibersegurança* Nacional. Já a *ciberdefesa*, diz respeito à realização de medidas e ações do estamento militar com a finalidade de resguardar a segurança cibernética das infraestruturas críticas do sistema nacional e daquela que forem designadas para a sua preservação, independentemente da origem da agressão.

O comitê de *cibergurança* é composto pela Segurança Civil e pela Defesa Nacional. Ou seja, há o Ministério de Modernização, há o Ministério de Segurança e há o Ministério da Defesa, conforme descrito na figura a seguir:

Figura 2 - Organização da *cibersegurança* na Argentina

Fonte: o autor, 2019.

A segurança perpassa todos esses órgãos. O nível que está sendo tratado é o do Ministério da Defesa - nível político. Neste nível, o que se faz é a *cibersegurança* das infraestruturas críticas da informação. Todos os dados das infraestruturas críticas usados atualmente nos estamentos do Estado ficam resguardados.

O Ministério de Modernização realiza a segurança cibernética da Diretoria Nacional de Infraestrutura Crítica de Informação e *Cibersegurança.* O Ministério de Segurança realiza a segurança cibernética da Gendarmeria Nacional, da Prefeitura Naval, da Polícia Federal e da Polícia de Segurança Aeroportuária. E o Ministério da Defesa faz a *ciberdefesa* de todas as infraestruturas críticas do instrumento militar. Tal atividade é realizada pelo Estado-Maior Conjunto.

O Sistema de *ciberdefesa* militar possui estrutura vertical, diferente do sistema de *cibersegurança*. A partir do presidente da nação, há o Ministro da Defesa, seguido pelo Estado-Maior Conjunto das Forças Armadas Argentinas, que atua no mesmo nível da Secretaria da Ciência e Tecnologia para Defesa. Sob a subordinação do Estado-Maior Conjunto, há o Comando Conjunto de *Ciberdefesa* (CCCD), que por sua vez estabelece comunicação com a Subsecretaria da *Ciberdefesa:*

Figura 3 - Organização da *ciberdefesa* na Argentina

Fonte: o autor, 2019.

O Brasil forneceu o conhecimento necessário para a Argentina criar o seu Comando Conjunto de *Ciberdefesa* (CCCD) em 2014. Em 2016, uma professora falou que a Alemanha considera o setor de *ciber* como sendo mais uma Força Armada.

Figura 4 - A *Ciberdefesa* no mundo

Fonte: o autor, 2019.

Quando a Argentina importou o conceito brasileiro que versa sobre o emprego de *ciberdefesa,* aplicou-se a mesma lei de defesa nacional e a lei de segurança interior. Mas o que aconteceu no espaço cibernético se não sabemos aonde vem o inimigo? O ambiente

cibernético é diferente do político, o que torna difícil a identificação da autoria de um ataque cibernético. Ou seja, a Argentina busca depreender sobre o espaço cibernético porque há um espaço cinza na esfera de responsabilidades entre a segurança interior e a defesa nacional, nas ações concernentes à defesa e à segurança cibernética.

A missão do CCCD é exercer a condução das operações de *ciberdefesa* de forma permanente para garantir as operações militares da Defesa Nacional, bem como garantir o cumprimento da sua missão principal, sempre alinhado com os preceitos estabelecidos no Planejamento Estratégico Militar. Suas principais funções são as seguintes:

Figura 5 - Funções do Comando Conjunto de *Ciberdefesa* na Argentina

Fonte: o autor, 2019.

A grande lição aprendida da Guerra das Malvinas é que tudo que a Argentina faz em termos de defesa é a nível conjunto, pelo que gera reflexos também na cibernética:

Figura 6 - Organização do Comando Conjunto de *Ciberdefesa* na Argentina

Fonte: o autor, 2019.

A estrutura do CCCD conta com dois grandes órgãos: o Centro de Operações Conjunto, que executa a atividade fim (monitoramento); e o Centro de Engenharia de

Conhecimento, que realiza a perícia do estudo. A pesquisa é desenvolvida nesse Centro de Engenharia e esse foi nosso crescimento. As infraestruturas críticas são os objetivos estratégicos do estamento militar, pelo que entra na órbita da *ciberdefesa.* O CCCD, por seu turno, estabelece os procedimentos operativos padrões para a preservação das infraestruturas críticas, além de estabelecer a doutrina para a execução da atividade.

Quando a Argentina recebeu o aporte brasileiro em 2014, os militares argentinos começaram a planejar o Comando Conjunto de *Ciberdefesa* no mesmo ano, vindo a organizar o mesmo já em 2015. Em 2016, o CCCD começou a fase de treinamento e a partir de 2017, o mesmo passou a ser empregado em operações:

Figura 7 - Evolução do Comando Conjunto de *Ciberdefesa* na Argentina

Fonte: o autor, 2019.

Haja vista que a cibernética não funciona isoladamente, a Argentina procura fortalecer a cooperação regional. Dessa forma, o país está incrementando as relações bilaterais, principalmente com o Chile, Brasil, Colômbia e Alemanha. Ou seja, as questões bilaterais são importantes para criar e promover maior cooperação multilateral necessária para a realização de ações nesse tipo de ambiente.

A *ciberdefesa* na Argentina possui quatro pilares, a saber: 1) pilar marco legal; 2) pilar recursos humanos; 3) pilar estruturação estratégica; e o 4) pilar infraestrutura ciência e tecnologia. O aspecto central está baseado na adequação, uma vez que sempre as forças precisam se adequar ao ambiente das operações, que está em constante e rápida transformação. Dessa feita, a visão estratégica do Centro Conjunto de *Ciberdefesa* é criar estratégias de coordenação entre os pilares e elaborar a doutrina cibernética militar e civil na Argentina, conforme sintetizado a seguir:

Figura 8 - Visão estratégica do Comando Conjunto de *Ciberdefesa* na Argentina

Fonte: o autor, 2019.

No setor cibernético, como a Argentina carece de mão de obra especializada em cibernética, constata-se que os recursos humanos também constituem o principal problema. Quando se observa o Brasil, nota-se que o mesmo também possui os mesmos problemas.

A tríplice hélice (Estado - universidade - oranização privada) é buscada o tempo todo na Argentina. Por exemplo, atualmente há militares argentinos fardados estudando e dando aulas nas universidades, da mesma forma que há universitários realizando estágios em organizações militares do Exército Argentino. Também há profissionais e empresários trabalhando junto com os militares, da mesma forma que há militares fardados ocupando espaços nas empresas e profissionais do setor civil trabalhando no Centro Conjunto de *Ciberdefesa*. Acredita-se que procedendo dessa forma, a gestão do conhecimento poderá funcionar.

Interessante pontuar que todas as províncias da Argentina são autônomas, ou seja, cada província tem sua própria constituição. Em suma, cada província pode ou não receber e aceitar as questões próprias dos estamentos militares. Para que todo mundo fale a mesma língua, é preciso que haja coordenação e cooperação entre as regiões nacionais e a capacitação da *ciberdefesa*. Neste aspecto, o Brasil é bem melhor desenvolvido e se encontra em estágio bem mais avançado do que a Argentina.

Finalmente, a infraestrutura, a ciência e a tecnologia requerem a sinergia das capacidades nacionais e da inovação baseada em capital humano. Nesse ínterim, procuramos sempre atuar junto com as universidades, com o objetivo de fomentar a

capacitação intelectual dos universitários. Estamos sempre buscando criar o nosso próprio sol e o nosso próprio calor. Em outras palavras, a Argentina está tentando conquistar o ciclo necessário de tecnologia por meio da aliança estratégica com o Brasil (transferência de tecnologia) e da aliança estratégica com a Alemanha.

A Diretoria de *Ciberdefesa* do Exército Argentino (DCEA) consiste num estamento menor, de nível tático, que funciona no marco da organização do Exército Argentino. Convém ressaltar que as outras Forças Armadas (Marinha e Força Aérea) também possuem órgãos congêneres. A finalidade da DCEA é assegurar o livre acesso ao espaço cibernético de interesse militar e oferecer resposta adequada ante as ameaças e agressões que possam afetar as infraestruturas críticas da força. Essa diretoria atende a proteção das infraestruturas críticas que foram entregues ao Exército Argentino. Sua estrutura é composta conforme organograma abaixo:

Figura 9 - Organização da Diretoria de *Ciberdefesa* do Exército Argentino

Fonte: o autor, 2019.

Dessa forma, trago duas questões que considero um ganho: 1) a criação, a partir da realidade geográfica da Argentina de uma Rede Técnica de Oficiais de *Ciberdefesa* (RTOC); e 2) a criação do Grupo de Resposta a Emergências e Incidentes de *Ciberdefesa* (GREIC).

A finalidade da RTOC é oferecer resposta adequada e imediata diante de um ataque ciernético. Para isso, conta com pessoal designado para cumprir funções específicas em cada Organização Militar dentro do campo de interesse de *ciberdefesa.* Já o GREIC, se destina a prevenir ou mitigar os efeitos das ameaças cibernéticas e impedir que as mesmas se propaguem.

A Argentina é um país grande com pouca população, possui infraestrutura nacional não muito desenvolvida, pelo que necessita de uma estrutura de proteção maior.

Diante dessa realidade, a figura a seguir apresenta o desdobramento do GREIC em território argentino. Em síntese, cada bolinha representada na figura a seguir já tem um GREIC em condições de fazer frente a possíveis emergências:

Figura 10 - Desdobramento da RTOC e dos GREIC no território argentino

Fonte: o autor, 2019.

3. Conclusões

Pelo que foi verificado, constata-se que a grande diferença entre Brasil e Argentina reside no nível tático. Quando a Argentina fala em segurança informática, o Brasil fala em guerra cibernética. São conceitos completamente distintos, mas a aplicação é a mesma. Diferente do Brasil, as Forças Armadas Argentinas consideram a segurança informática no nível tático.

A existência de órgãos de *ciberdefesa* nos níveis tático, operacional e estratégico, favorece o estabelecimento de uma relação direta entre os níveis cibernéticos e a sua condução. O CCCD é a nível operacional e orienta os esforços das Diretorias de *Ciberdefesa* de cada Força Armada. Quando a gente faz o trabalho conjunto e decide atuar com o Brasil, o principal problema está nos níveis, enquanto um é tático, o outro é operacional. A evolução da *ciberdefesa* na Argentina passa, obrigatoriamente, pela contribuição brasileira nesse esforço e o RTOC e o GREIC são ferramentas muito úteis para otimizar o funcionamento do sistema.

Muito obrigado!

CIBERSECURITY E INFRAESTRUTURAS CRÍTICAS

André Clark*

1. Introdução

Bom dia a todos e a todas.

Eu quero agradecer a oportunidade de estar na Escola de Comando e Estado-Maior do Exército com vocês. Como brasileiro, como CEO (*Chief Executive Officer*) de uma empresa que está há cerca de 150 anos presente no Brasil e obviamente como alguém que acredita profundamente na interação estratégica entre a Defesa Nacional, o mundo privado e a sociedade. Acredito que é papel de todo líder empresarial e de todos os brasileiros de se engajarem nas grandes questões de segurança nacional e de defesa nacional.

O mundo do *ciberespaço* e o mundo das infraestruturas são uma área de altíssima responsabilidade para todos nós. O foco da minha apresentação é tentar fazer a ligação do papel que exerce um CEO que conduz o dia a dia dos negócios de uma empresa e do papel que um administrador de uma empresa exerce no Brasil com as questões relativas à segurança nacional e à defesa nacional na parte atinente ao *ciberespaço*.

O mundo do *cibersecurity* e as questões éticas concernentes ao uso da tecnologia talvez sejam um dos maiores desafios da humanidade nos dias atuais. Eu costumo colocar o desafio da *cibersegurança* quase no mesmo nível do desafio com as questões afetas ao aquecimento global e à redução da emissão de carbono. Isso se deve porque os dois desafios citados possuem características muito semelhantes e a sociedade só consegue resolver esses problemas por meio de muita colaboração, ou seja, é um desafio de natureza complexa, que precisa ser enfrentado de forma coletiva, pois é elemento central para o desenvolvimento da humanidade nas próximas décadas.

2. Desenvolvimento

A *Siemens* conta atualmente com quase 380 mil colaboradores espalhados no mundo. O faturamento anual da empresa está na ordem de 83 bilhões de euros. O grande foco da *Siemens* é rapidamente se tornar a maior empresa de *software.* Hoje, a *Siemens* está situada entre os cinco maiores produtores de *software* do planeta:

Figura 1 - Dados gerais da *Siemens*

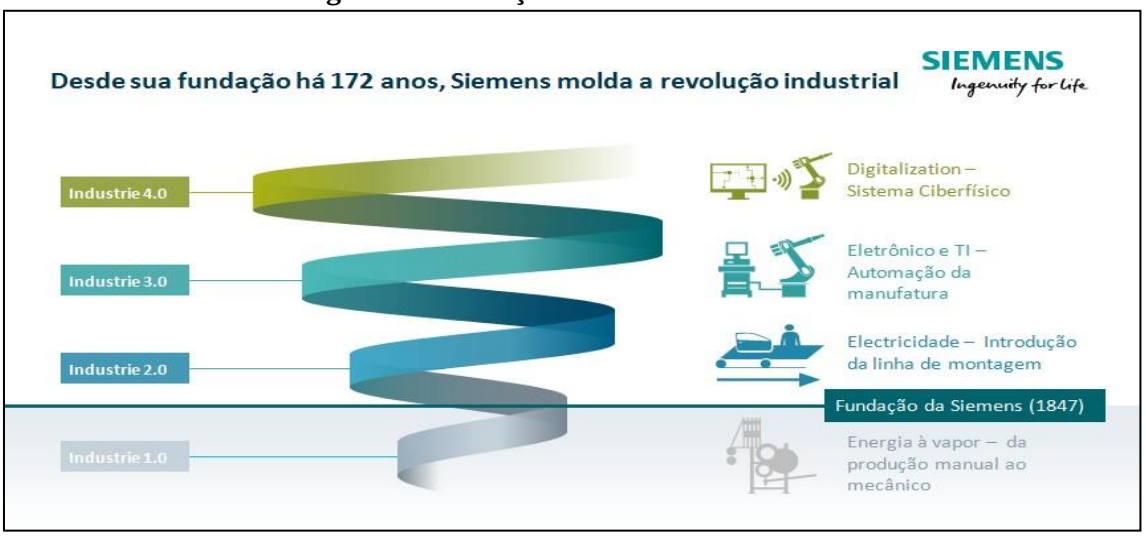
* Presidente da *Siemens* do Brasil.

Fonte: o autor, 2019.

O Brasil segue a tendência mundial e também registra crescimento no mundo do *software*, principalmente dos que estão em máquinas, na base do sistema produtivo e no sistema de infraestruturas. A *Siemens* trabalha com saúde, com mobilidade urbana, com grandes sistemas de gestão, distribuição e geração de energia.

A indústria 4.0 não é algo novo. A grande diferença nos dias atuais é que é um sistema absolutamente integrado, cibernético e digitalizado. Dessa forma, para um país que procura produtividade (como é o caso do Brasil), isso se torna essencial para ficar em condições de enfrentar a próxima onda de desenvolvimento.

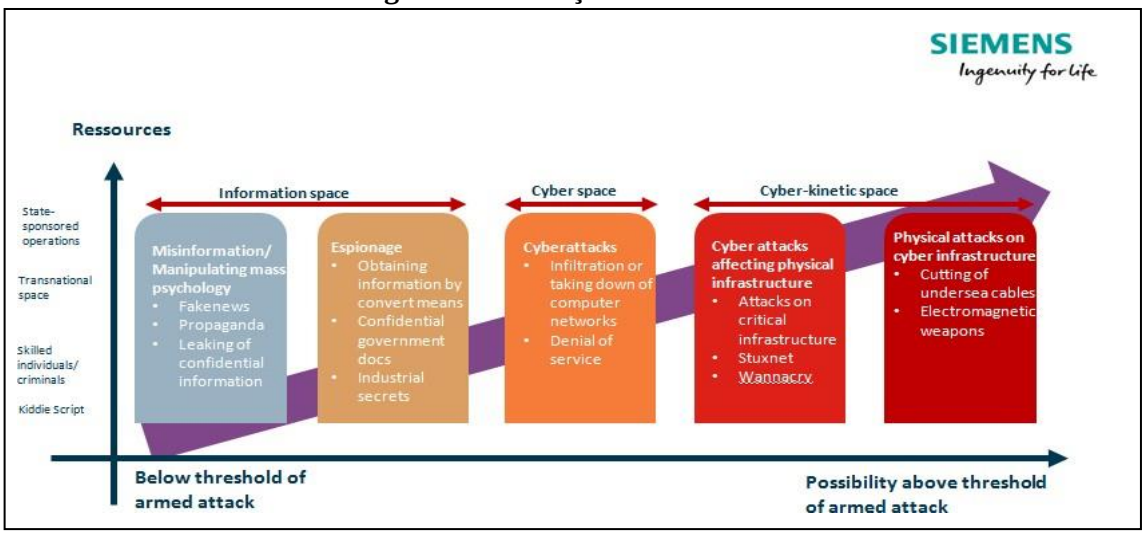
Figura 2 - Evolução histórica da *Siemens*



Fonte: o autor, 2019.

O gráfico a seguir foi exposto numa conferência de *cibersegurança* organizada pela fundação *Konrad Adenauer*. Ele apresenta um modelo que a ONU tem utilizado e que eu gosto de usá-lo, conforme descrito a seguir:

Figura 3 - Ameaças cibernéticas



Fonte: *Konrad Adenauer Foundation*, 2019.

O eixo x contém o tamanho e o tipo da ameaça, ou seja, a ameaça cresce à medida que caminha para direita, variando desde ameaças abaixo do patamar de um ataque armado, até ameaças acima do patamar de um ataque armado. Já o eixo y contempla os recursos envolvidos com a ameaça. Podemos ter recursos que são patrocinados por Estados, até inciativas cibernéticas realizadas por um simples menino ou menina curiosa querendo mostrar a sua capacidade de fazer coisas.

A heterogeneidade é importante porque se relacionam entre si. Um Estado pode tranquilamente contratar um indivíduo criminoso, aspecto que deixa a *Siemens* bastante preocupada, pois um ataque no espaço de informação tem consequências sérias.

O Brasil vive um ataque à nossa democracia, seja lá qual for a origem, o programa, o tamanho, a profundidade da investigação dessas coisas, simplesmente disseminar informação e manipular a opinião pública é um ataque a nossa democracia.

À medida que a sociedade avança, cresce a possibilidade da ocorrência de uma invasão em outros *ciberespaços*, em especial os ataques às infraestruturas físicas. Os casos envolvendo o *Stuxnet* e o *Wannacry* são exemplos clássicos de ataques às infraestruturas físicas e que geraram enormes danos à sociedade, em particular nos locais onde eles foram inseridos. O problema é que esse tipo de guerra não há limites, não há acordo de Genebra para a guerra cibernética. E as consequências podem ser devastadoras para as nações. E por isso, atualmente a humanidade discute quais são os limites de uma guerra nesse ambiente.

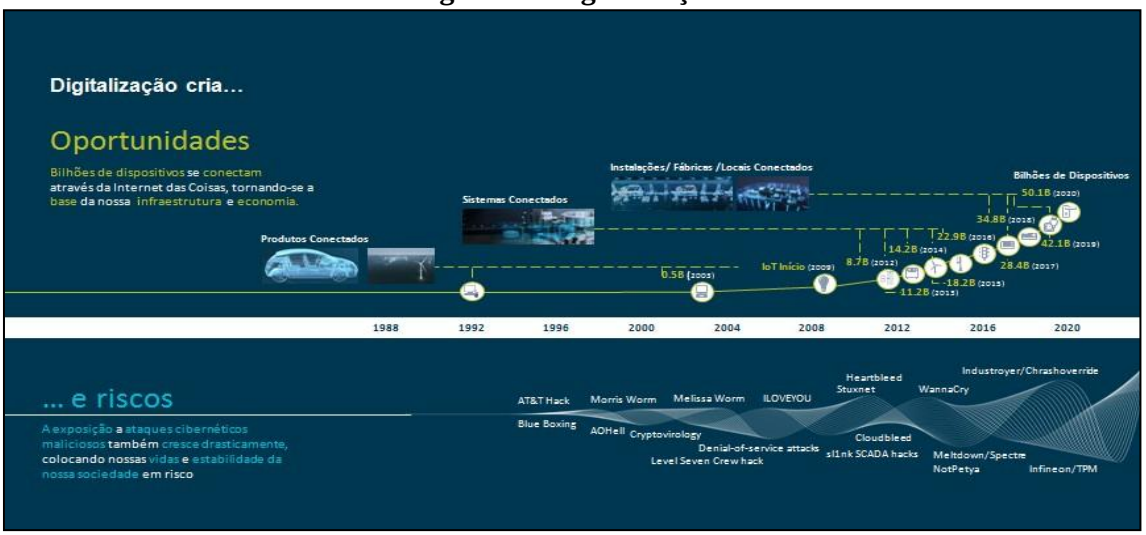
Nessas discussões, há algumas coisas interessantes. Já se estima que algo em torno de 1% a 2% do PIB da Coreia do Norte é composto por ataques cibernéticos empregados para arrecadar recursos financeiros para o país. Ou seja, os ataques cibernéticos fazem

parte da receita de um ente nacional para financiar os seus próprios propósitos. Outro exemplo recai no enfraquecimento das Nações Unidas. No atual ambiente multipolar e geopolítico no planeta, a instituição se encontra muito enfraquecida. Alguns entes de Defesa Nacional começam a perceber que o ambiente atual é sem regras e o que funciona é a colaboração (*trust).*

O FBI norte-americano e algumas agências europeias conduziram diversas discussões afetas à proteção cibernética de instituições públicas e privadas. O que se fala nessas reuniões é que a proteção cibernética deve ser feita tanto em instituições nacionais, como em empresas do setor privado, como a *Siemens*. Os Estados Unidos da América (EUA) esperam várias colaborações de empresários no mundo do *ciberespaço*. Como exemplo, um CEO brasileiro pode ser convidado para uma reunião específica sobre defesa cibernética nos EUA, e nesta reunião o brasileiro pode ser cobrado de autoridades norte-americanas sobre colaborações que podem ser efetuadas nessa área.

Isso muda muito a equação e a forma de relação entre os entes de defesa de um país e o ambiente produtivo da sociedade. Eu particularmente fiquei impressionado com essa experiência até cair a ficha de que o mundo do *ciberespaço* é um jogo absolutamente formal e informal de colaboração e de construção de confiança. Assim como ocorre no ambiente norte-americano, o Brasil pode ter gente formada na área de defesa trabalhando nas empresas mais estratégicas do país, seja ela de capital nacional ou de capital internacional, como ocorre normalmente em outros países.

Figura 4 - Digitalização



Fonte: o autor, 2019.

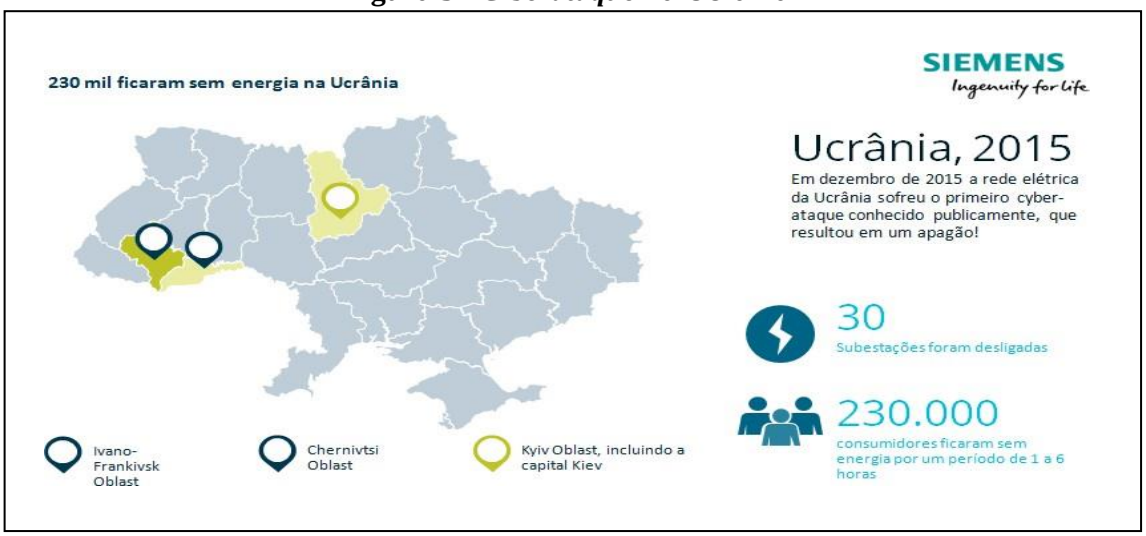
O mundo do *ciberespaço* irá gerar oportunidades importantes na expansão da rede de colaboração entre o mundo da defesa e o mundo civil (do dia a dia dos negócios), em especial no ambiente das infraestruturas críticas.

A digitalização gera um cenário onde há bilhões de dispositivos integrados no planeta, pelo que os riscos aparecem com mais frequência. Um exemplo clássico é o *Wannacry*, um vírus relativamente simples, mas que é capaz de causar um grande estrago. O sistema elétrico brasileiro é absolutamente digital, está inteiramente situado nas nuvens. Pela capacidade técnica brasileira, o Brasil foi o único país do mundo capaz de desenvolver as tecnologias necessárias para gerenciar o sistema elétrico com esse nível de complexidade e atualmente o mesmo consegue exportar esse tipo de tecnologia.

O que a *Siemens* tem defendido é que os recursos destinados à Pesquisa e Desenvolvimento sejam também destinados à proteção cibernética das infraestruturas críticas, pois isso trará capacidade na geração de serviços cibernéticos, os quais podem se tornar uma fonte adicional de recursos também. Ou seja, é uma agenda positiva, pois dá capacidade brasileira nessa área.

Em 2005, houve um caso de ataque cibernético na Ucrânia. Em dezembro de 2005, a rede elétrica da Ucrânia sofreu o primeiro *ciberataque*, que resultou num apagão elétrico, conforme especificado a seguir:

Figura 5 - *Ciberataque* na Ucrânia



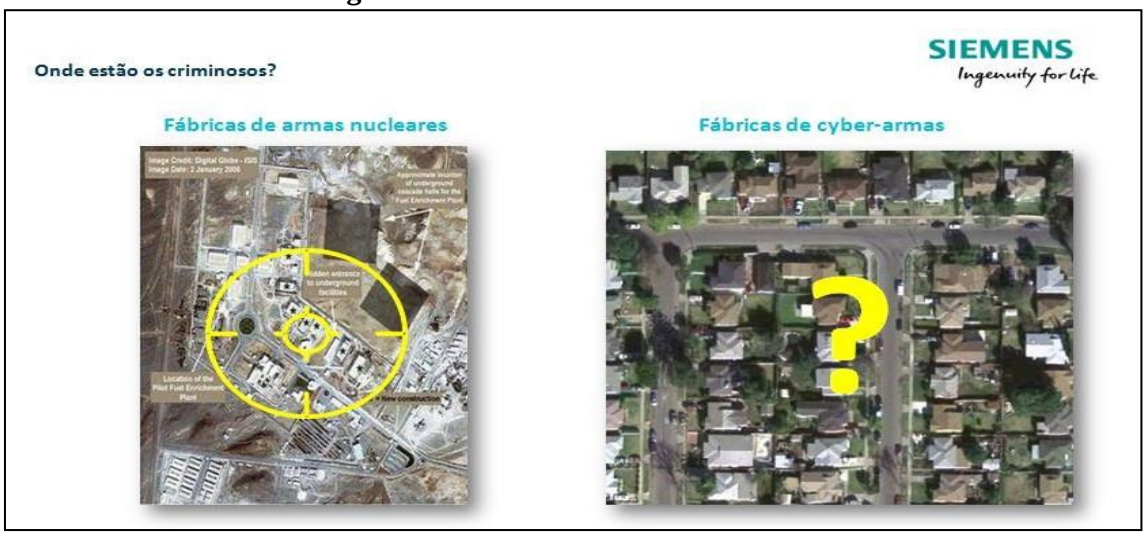
Fonte: o autor, 2019.

Devido a um ataque cibernético, cerca de 200 mil habitantes na Ucrânia ficaram sem energia elétrica durante várias horas. Não é difícil de acontecer isso no Brasil, na Argentina ou mesmo em *Manhattan*. Recentemente, uma falha num transformador apagou a cidade de Nova York e obviamente as hipóteses especuladas giraram em torno da precária manutenção e de um possível ataque cibernético.

Um aspecto interessante diz respeito à natureza do *cibercriminoso*. Como é o seu perfil? A fábrica de armamento nuclear necessita de um espaço geográfico de fácil identificação, já o *cibercriminoso* pode atuar em qualquer lugar. Dessa forma, a

cooperação é absolutamente necessária entre todos os entes interessados nesse jogo.

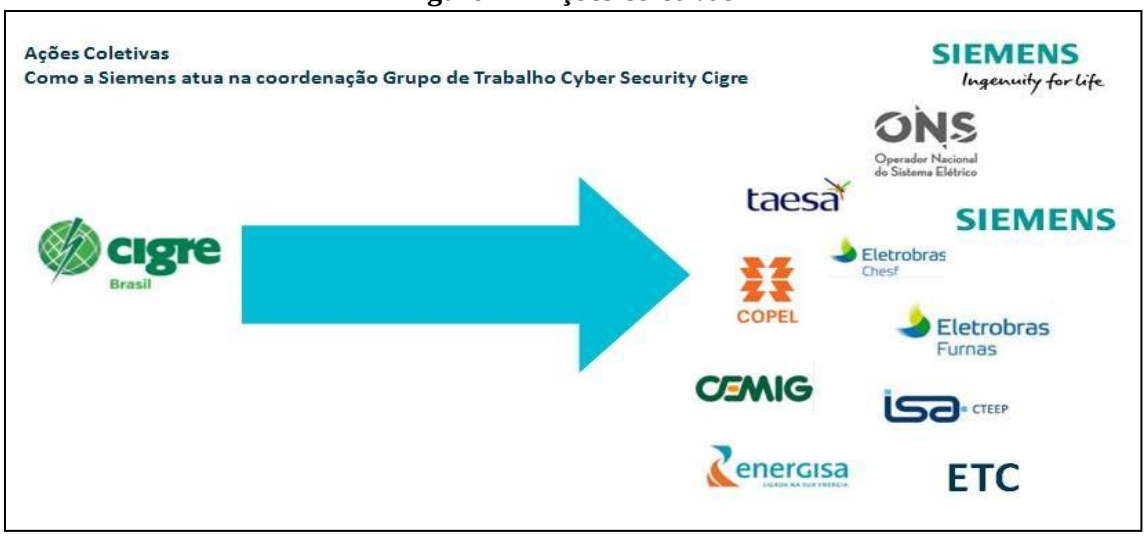
Figura 6 - Natureza do *cibercriminoso*



Fonte: o autor, 2019.

O CIGRE é uma associação que trabalha em prol do desenvolvimento do setor elétrico brasileiro, congregando todos os operadores nacionais em torno das questões referentes à defesa e segurança cibernética, conforme apresentado a seguir:

Figura 7 - Ações coletivas

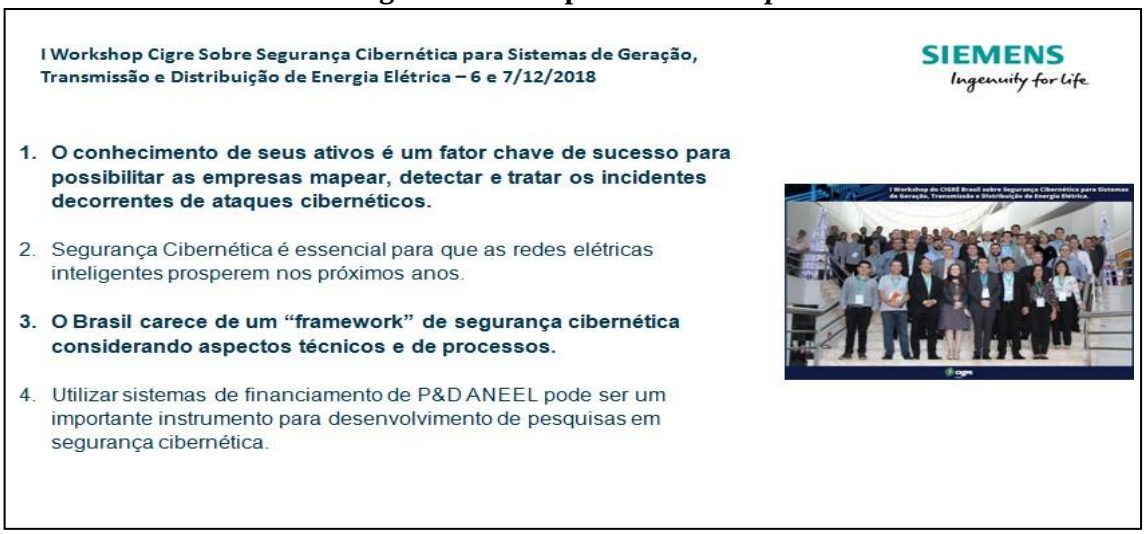


Fonte: o autor, 2019.

Obviamente a presença do Estado e das Forças de Defesa neste tipo de ambiente é essencial, pois delimitam as atribuições e colocam seus interesses e suas demandas nesse espaço. Mais do que isso, é também uma enorme possibilidade de geração de emprego, renda. O Brasil possui centros de tecnologia da informação bem capacitados. Ou seja, o Brasil é profundamente competitivo nessa área, pelo que é uma oportunidade.

A figura a seguir apresenta um *Workshop* que a *Siemens* está fazendo no sentido de conscientizar a população em geral, bem como difundir as oportunidades advindas do mundo cibernético.

Figura 8 - Exemplo de *Workshop*



Fonte: o autor, 2019.

3. Conclusões

Em termos globais, a *Siemens* está atuando sob a forma de *Charter of Trust* (carta de confiança), visando três objetivos importantes: 1) proteger os dados de indivíduos e empresas; 2) evitar danos a pessoas, empresas e infraestruturas; e 3) criar uma base segura para que a confiança em mundo conectado e digital possa criar raízes e crescer.

Se for empregada de forma inteligente, a gente acha que esse tipo de ação (Forças do Estado interagindo com as empresas no o dia a dia) talvez seja uma das melhores soluções para se proteger no mundo cibernético.

Muitíssimo obrigado!

CIBER ARENA (ABDI-BIOTIC)

Larissa de Freitas Querino*

1. Introdução

Bom dia a todos.

Meu nome é Larissa Querino e sou especialista em Indústria de Defesa e coordenadora de difusão tecnológica na Agência Brasileira de Desenvolvimento Industrial (ABDI). Queria agradecer a ECEME pelo convite, pois acho que é uma bela oportunidade trabalhar sobre um tema tão relevante que é a questão da segurança cibernética. A minha apresentação estará pautada pela exposição de números sobre o mundo cibernético. Ao final dela, será apresentada uma proposta, que é um projeto que a ABDI está desenvolvendo sobre um Centro de Segurança Cibernética voltado para a capacitação de recursos humanos.

A ABDI é uma instituição de direito privado sem fins lucrativos e de utilidade pública. Criada em dezembro de 2004, o propósito da ABDI é trabalhar com o governo na estruturação de políticas industriais, prestar subsídios e fazer a articulação dos atores para a política industrial.

Conforme descrito na figura a seguir, atualmente, a Agência Brasileira de Desenvolvimento Industrial está vinculada ao Ministério da Economia por contrato de gestão e trabalha em parceria com o setor público e com o setor privado, com foco voltado na competitividade, produtividade e inovação da indústria brasileira:

Figura 1 - Agência Brasileira de Desenvolvimento Industrial

Fonte: o autor, 2019.

* Coordenadora de Difusão Tecnológica da Agência Brasileira de Desenvolvimento Industrial (ABDI).

2. Desenvolvimento

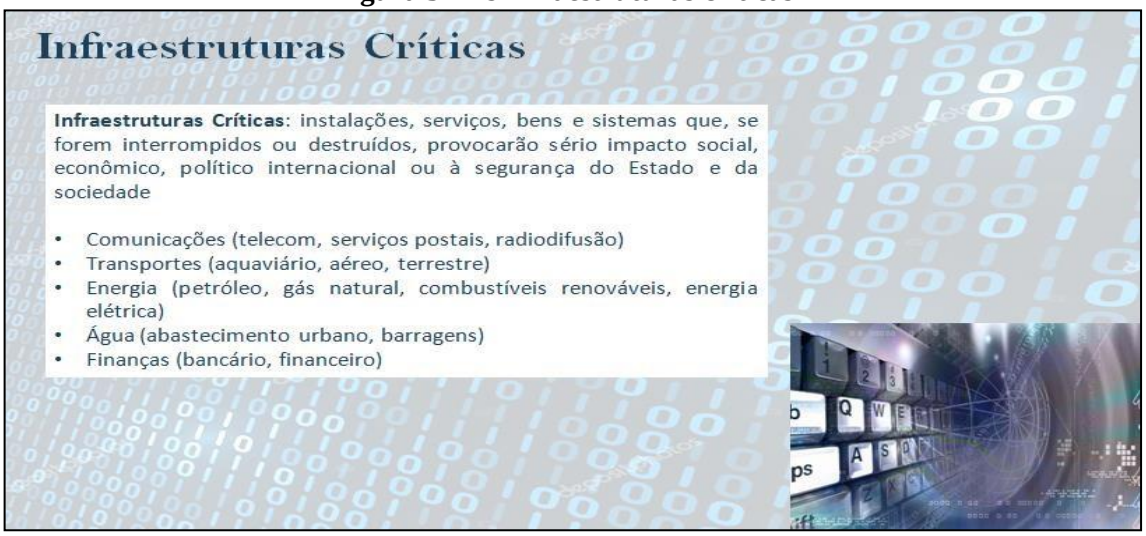
Não é novidade para ninguém que a economia está cada vez mais digitalizada. Ela depende dos sistemas, da conectividade, do uso de *internet* das coisas e nesse contexto, ressalta-se a importância da segurança cibernética, conforme descrito a seguir:

Figura 2 - Digitalização da economia

Fonte: o autor, 2019.

Nos dias atuais, há incidentes que param as linhas de produção, há incidentes que os dados dos clientes são vazados, etc. Isso traz impactos significativos nas atividades econômicas e sociais, pelo que se torna um cenário que precisa ser endereçado de forma específica nas pesquisas realizadas na ABDI. Nesse sentido, o que a ABDI notou é que além da cooperação (atuação em parceria), há um *gap* na formação de recursos humanos especializados nessa área.

Figura 3 - As infraestruturas críticas



Fonte: o autor, 2019.

As infraestruturas críticas englobam os serviços de comunicações, de transportes, de energia, de água, sistema financeiro e bancário.

Então o que são os ataques cibernéticos? Os ataques cibernéticos podem ser definidos como atividades maliciosas conduzidas contra organizações, por meio de sua infraestrutura de tecnologia da informação, via redes internas, externas ou a *internet*. Incluem, ainda, ataques contra sistemas de controle industrial. Entre 2016 e 2017, o mundo presenciou um aumento exponencial no número de ataques a *IoT* (600 %). O Brasil está entre os cinco principais países de origem desses ataques de *IoT* no mundo.

A *Elbit Systems* fez um estudo e mapeou a média de dias utilizados para identificar e conter os ataques cibernéticos. Normalmente o ataque acontece por mais de 200 dias sem que a empresa se dê conta com o que está acontecendo e a partir do momento que a empresa toma conhecimento de que está sendo atacada, ela leva mais 70 dias para combatê-lo.

A nova realidade conjuntural do mundo cibernético se fez refletir também no setor financeiro, gerando um aumento enorme nos custos e nos gastos relacionados à segurança cibernética. O custo anual dos crimes cibernéticos no globo foi estimado em 608 bilhões de dólares, o que equivale a 0,8% do PIB mundial. Por sua vez, as empresas gastam anualmente com segurança cibernética, algo em torno de 100 bilhões de dólares:

Figura 4 - Custos e gastos da segurança cibernética

Fonte: o autor, 2019.

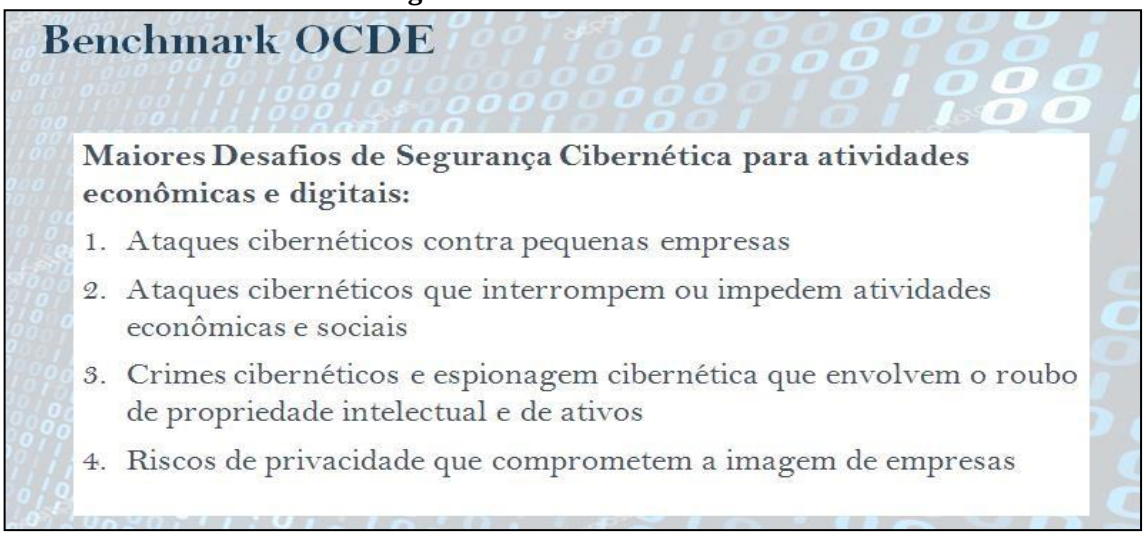
O índice global de *cibersegurança* (criado pela Organização Internacional de Telecomunicações) mensura os níveis de *cibersegurança* dos países do globo terrestre. Neste índice, o Brasil está na 70ª posição, o que é péssimo. No continente americano, o Brasil ocupa a 6ª posição. No que concerne à ocorrência de crimes cibernéticos, o Brasil ocupa a 2ª posição, com 78% desses crimes cibernéticos sendo originados dentro do próprio país.

Interessante destacar que 45% das empresas do mundo não estão preparadas para

combater esses crimes e que 62 bilhões de usuários são afetados anualmente, causando prejuízo e da ordem de 22,5 bilhões de dólares.

A OCDE analisou alguns países do mundo para saber como eles lidam com a segurança cibernética e quais são as ações que eles costumam tomar para garantir um ambiente mais seguro e fez um *Benchmark* elencando os maiores desafios de segurança cibernética para o desenvolvimento da atividade econômica e digital nos dias atuais:

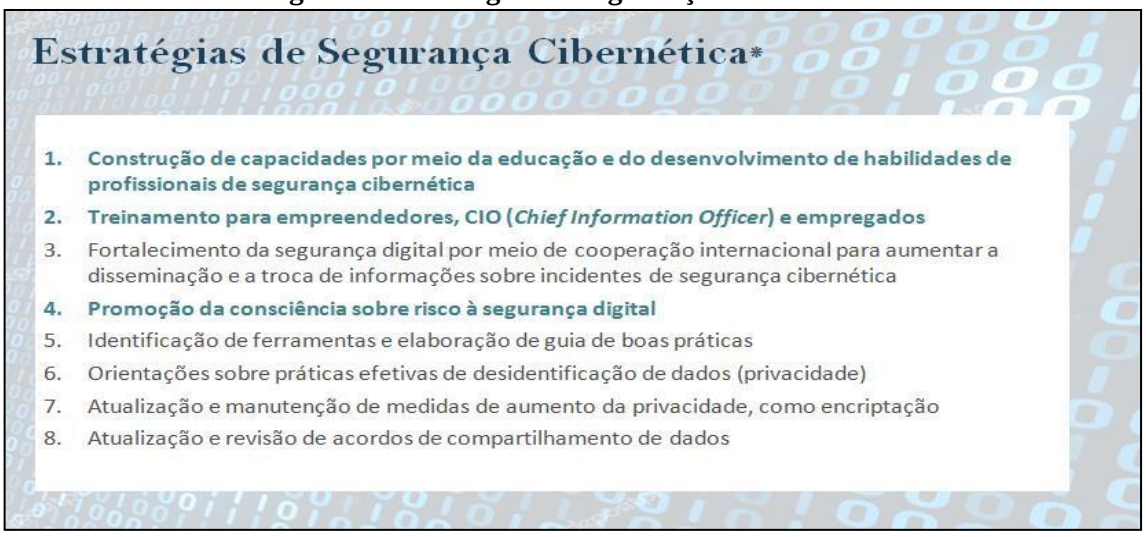
Figura 5 - *Benchmark* OCDE



Fonte: o autor, 2019.

E quais seriam as estratégias de segurança cibernética adotadas pelos países da OCDE?

Figura 6 - Estratégias de Segurança Cibernética



Fonte: o autor, 2019.

As quatro primeiras estratégias estão muito voltadas para a proposta atual da ABDI, qual seja: qualificação de recursos humanos.

E aí a gente entra um pouco na proposta da ABDI, que tem uma relação muito próximo também com o Comando de Defesa Cibernética do Brasil. No final de 2018, o

presidente da ABDI esteve em Israel e ficou muito impressionado com o que viu no país israelense. Nesta ocasião, a ABDI foi convidada para acompanhar o exercício de *Blue Team Resilience,* que é semelhante ao Guardião Cibernético conduzido no Brasil. Além disso, nós visitamos empresas em Israel que prestam esse serviço para outras empresas de uma forma mais efetiva. Na volta ao Brasil, viemos pensando em como a ABDI poderia atuar nesse segmento e contribuir para a formação de recursos humanos dedicados exclusivamente para segurança cibernética no Brasil. Constatamos também que o Brasil não possui um curso de graduação em segurança cibernética. O que há no país são cursos espalhados em capacitações realizadas pelas próprias empresas.

Outra coisa interessante é que na Coréia do Sul, as crianças que possuem seis anos já começam a lidar com a questão da segurança cibernética, ou seja, já começam a ser educados no mundo cibernético. Em suma, há uma quebra de paradigma cultural que precisa ser feita no Brasil.

3. Conclusões

Diante dessas considerações, a ABDI está propondo a criação de um centro segurança cibernética: *Cyber* Arena.

Figura 7 - Objetivos do Projeto *Cyber* Arena

Fonte: o autor, 2019.

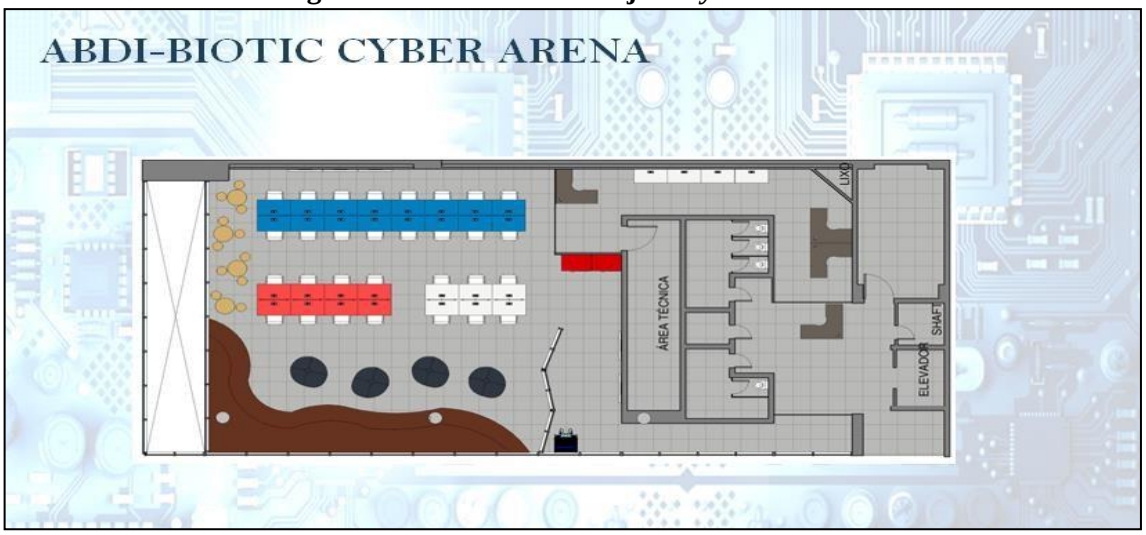
A ABDI está criando esse centro com base no modelo de *Cyber Range,* que é um ambiente virtualizado para treinamento, experimentação, avaliação de vulnerabilidades, trabalho em grupo, *feedback* em tempo real, experiência *on the job*, teste de novas ideias e solução de problemas cibernéticos, onde ataques cibernéticos são realizados em réplica de ambiente real de operação de uma organização, de maneira segura, controlada e confiável. Esse é o modelo que as empresas em geral adotam para fazer a capacitação. É

real e simula todas as estruturas de uma empresa ou de uma infraestrutura crítica que possam ser atacadas.

A ABDI também fez no final do ano passado em Brasília-DF, um exercíco chamado de *Capture the Flag* (CTF), que é um exercício um pouco mais simples de segurança cibernética. A proposta foi interessante porque possibilitou o mapeamento dos grupos que estão trabalhando nisso em Brasília-DF. Esse exercício também contou com a presença do Comando de Defesa Cibernética e dos alunos do Instituto Militar de Engenharia (IME), que são extremamente capacitados nesse assunto.

Prevista para ficar instalada no parque tecnológico do *Biotic*, essa é mais ou menos a estrutura do *cyber* arena:

Figura 8 - Estrutura do Projeto *Cyber* Arena



Fonte: o autor, 2019.

O projeto prevê uma área total de 350 m2. Haverá áreas para treinamento do *Blue Team Resilience*, da atuação do *Red Team* e do *White.* Além disso, haverá espaço também para a realização de exercícios mais simples e uma área de observação para quem quiser acompanhar o exercício. A estrutura da ABDI-BIOTIC *cyber* arena é sob o formato aberto, pois a proposta é que seja de fato um espaço de compartilhamento de conhecimento e de troca de experiências.

Os exercícios que a ABDI está pensando fazer são os *Blue Team Resilience*, o *Capture the Flag* e a capacitação em ataque/defesa cibernética e os serviços que a ABDI vai tentar modular para uma oferta futura são os testes de segurança (Zero *Day*, *Malwares* e vírus), Testes de Resiliência e *Harderning* e avaliação de vulnerabilidades cibernéticas.

Obrigada a todos e me coloco à disposição para qualquer pergunta!

LABORATÓRIO DE SEGURANÇA CIBERNÉTICA EM AMBIENTE DE TECNOLOGIAS DE INFORMAÇÃO E AUTOMAÇÃO APLICADA EM SISTEMAS ELÉTRICOS

Tenente-Coronel Antônio Eduardo Carrilho da Cunha*

1. Introdução

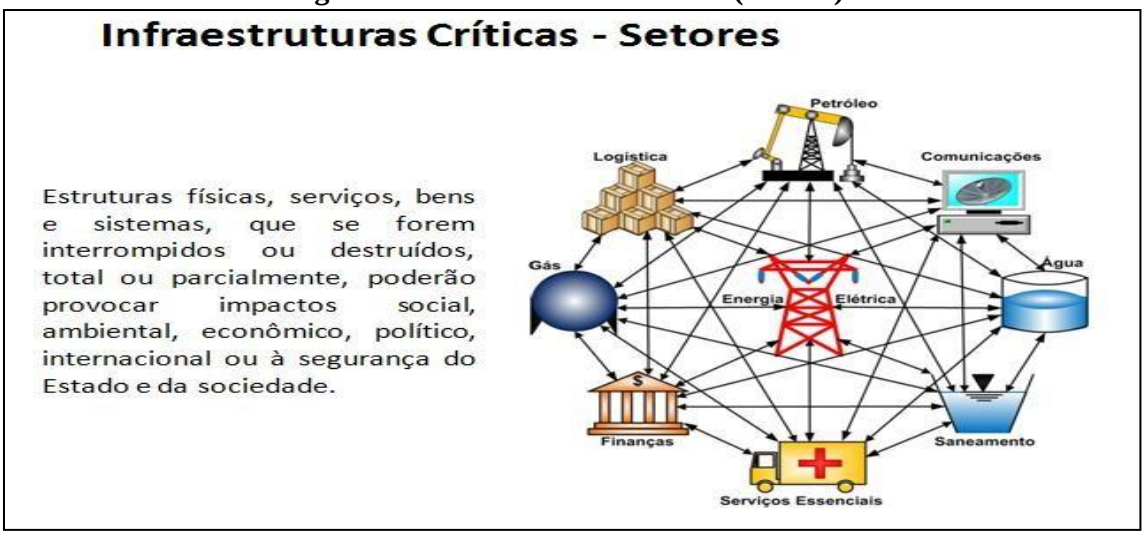
Senhores, bom dia.

Estou muito honrado com o convite feito pela Escola de Comando e Estado-Maior do Exército para participar do 21º Ciclo de Estudos Estratégicos. A minha apresentação buscará focar no laboratório que está sendo montado pelo Exército Brasileiro em parceria com Itaipu. O nome do mesmo é Laboratório de Segurança Cibernétia em Ambiente de Tecnologias de Informação e Automação aplicada em Sistemas Elétricos (LaSC).

2. Desenvolvimento

As infraestruturas críticas não estão atuando de forma isolada no mundo. Pelo contrário, todas elas estão interligadas, cabendo ao setor elétrico o papel de epicentro das ligações. Ou seja, se o setor elétrico cair, fatalmente os outros também cairão.

Figura 1 - Infraestuturas Críticas (setores)



Fonte: o autor, 2019.

Ano passado tivemos um problema numa infraestrutura crítica que não envolveu diretamente o espaço cibernético, mas que parou o Brasil. Quando o espaço cibernético está no centro, tudo que envolve o setor cibernético se torna sensível e complexo.

---

* Doutor em Enganharia Elétrica e Coordenador do Programa de Pós-graduação em Engenharia de Defesa, do IME.

A figura a seguir mostra os domínios do sistema elétrico, os quais são interligados pela energia elétrica e por cabos de comunicação, que se encontra cada vez mais no espaço cibernético:

Figura 2 - Domínios do setor elétrico

Fonte: o autor, 2019.

O espaço cibernético é um ambiente permanente de mudança e cada vez mais está presente na vida das pessoas. Para um empresário obter mais faturamento, fatalmente o mesmo deverá automatizar os seus serviços e isso o tornará mais vulnerável e suscetível aos ataques cibernéticos.

Dessa forma, torna-se imperioso o fortalecimento de uma cultura de segurança cibernética e de uma atuação estratégica que considere as suas dimensões (tecnologias utilizadas, aspectos sociais e inter-relacionamento).

Nas questões afetas à segurança do sistema de energia elétrica do Brasil, nota-se que o operador nacional do sistema é responsável para propor as regras de operação das instalações de transmissão da rede básica do SIN, a serem aprovadas pela Agência Nacional de Energia Elétrica (ANEEL). No que concerne à ITAIPU, verifica-se que a mesma está renovando completamente a sua automação, ou seja, um processo que deve durar algo em torno de 14 anos. O que isso acarretará? Certamente ocorrerá um aumento da vulnerabilidade do sistema.

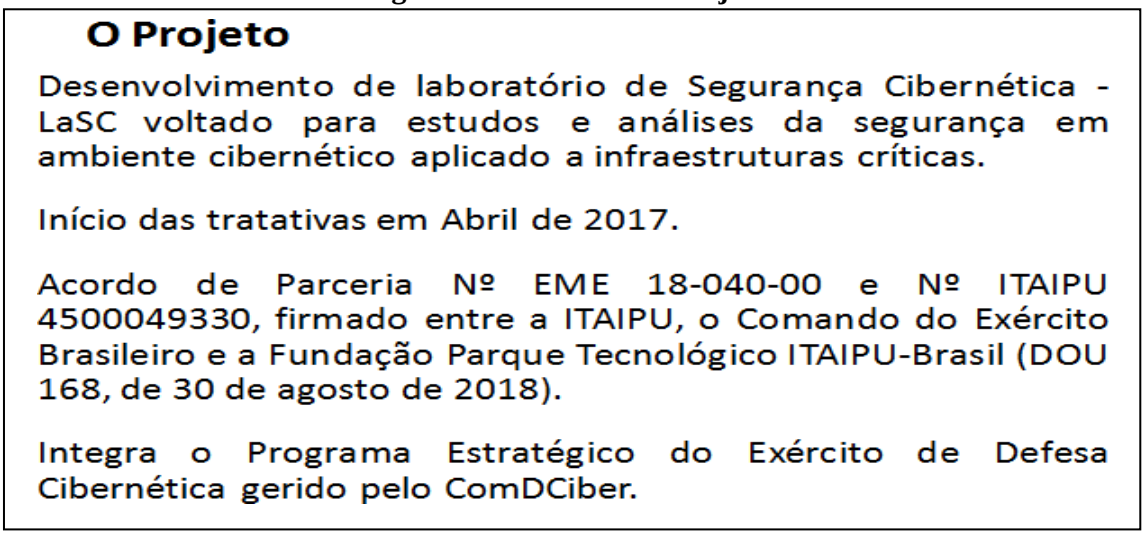
A solução para diminuir a vulnerabilidade do sistema foi elaborar um sistema interligado de segurança integrada. O que interliga toda a parte interna do sistema é a segurança em profundidade, que envolve a camada de gerenciamento, a camada de supervisão e monitoramento, a camada de produção e controle de processos e a camada de processos. Essa arquitetura está representada de acordo com a figura a seguir:

Figura 3 - Sistema Interligado de Segurança Integrada

Fonte: o autor, 2019.

Recordo que o espaço cibernético tem efeito fortíssimo no mundo cinético. A preocupação do ONS e dos agentes está na segurança da interligação, mas tem que haver também uma preocupação do agente na segurança em profundidade (níveis 0, 1, 2, 3). Nesse contexto, o Laboratório de Segurança Cibernétia em Ambiente de Tecnologias de Informação e Automação aplicada em Sistemas Elétricos está surgindo para que essas ações de segurança sejam complementares e integradas.

Figura 4 - Histórico do Projeto



Fonte: o autor, 2019.

O projeto (LaSC) se encontra sob o guarda-chuva da Estratégia Nacional de Defesa (END), que definiu o Exército Brasileiro como responsável pela defesa cibernética, que por sua vez designou o Comando de Defesa Cibernética como o gestor do programa estratégico de defesa cibernética e que delegou ao Instituto Militar de Engenharia (IME), a responsabilidade pela condução de projetos de pesquisas voltados para a área cibernética.

O IME atua na captação de parcerias para contribuir no desenvolvimento do projeto (nacionais e internacionais, academia, setor público e setor privado). A figura a seguir sintetiza as parcerias efetuadas pelo IME:

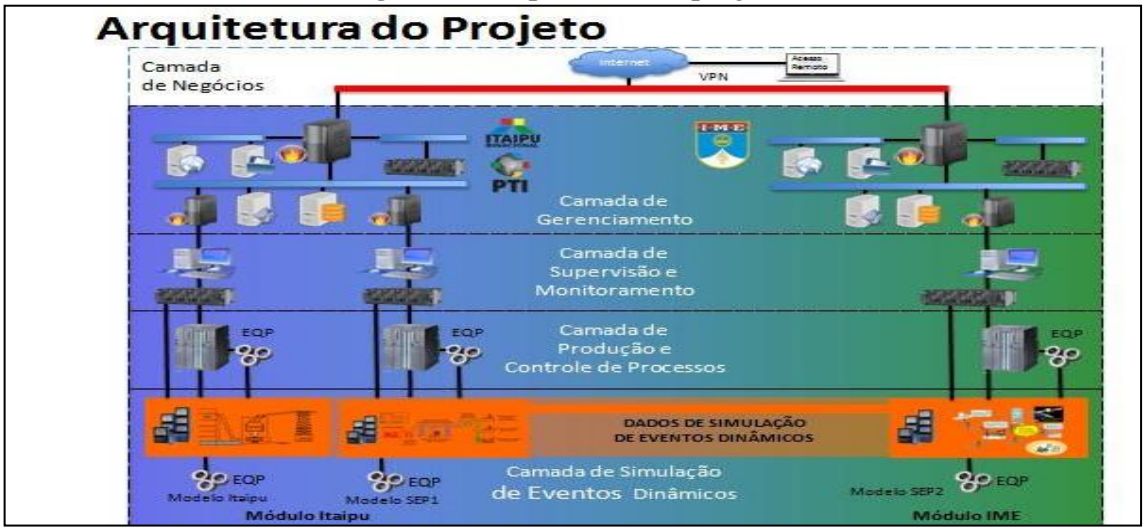
Figura 5 - Parcerias do IME

Fonte: o autor, 2019.

O objetivo do projeto é ser um instrumento que permite gerir de forma mais eficiente a continuidade do fornecimento de energia no país. Se houver um incidente, a meta é que haja uma resposta ao incidente.

A figura a seguir apresenta as camadas que serão implementadas no escopo do projeto. Haverá dois laboratórios físicos: um laboratório em Itaipu e outro laboratório no IME. Nessa arquitetura, será simulada a rede corporativa dos dois lados e a parte de supervisão e monitoramento (SCADA). Haverá também a simulação de um sistema elétrico, como se fosse uma usina geradora, uma distribuidora, todas em cima do *software* chamado RTDS, conforme apresentado a seguir:

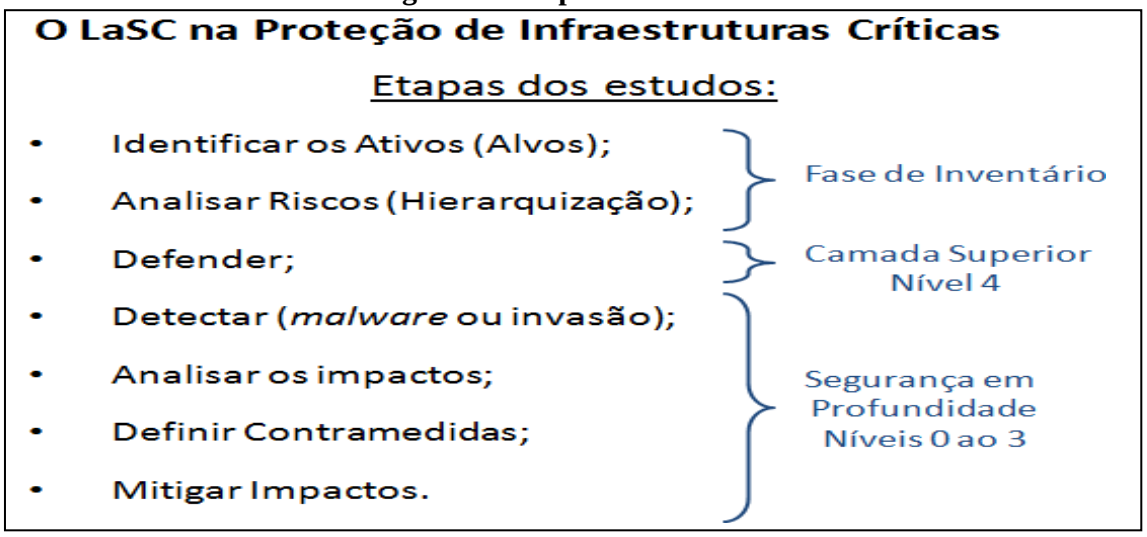
Figura 6 - Arquitetura do projeto



Fonte: o autor, 2019.

O projeto possui as seguintes etapas:

Figura 7 - Etapas dos estudos



Fonte: o autor, 2019.

Dentre os diversos produtos que o LaSC pode oferecer, destaca-se a certificação de equipamentos. No que diz respeito aos recursos aplicados, observa-se que 60,2% do total foram destinados à aquisição de equipamentos TA e 9,7% foram destinados aos equipamentos TI. No que diz respeito às parcerias realizadas, destacam-se as realizadas com o COPPE-UFRJ (pesquisas conjuntas na área de automação/cibernética), com o ONS (cooperação técnico-científico e interligação de simuladores RTDS e OPAL) e com o CEPEL (cooperação técnico-científica e do uso do programa SAGE).

Importante pontuar que o projeto também está buscando uma integração com os centros de simulação existentes no centro-sul do país, conforme apresentado a seguir:

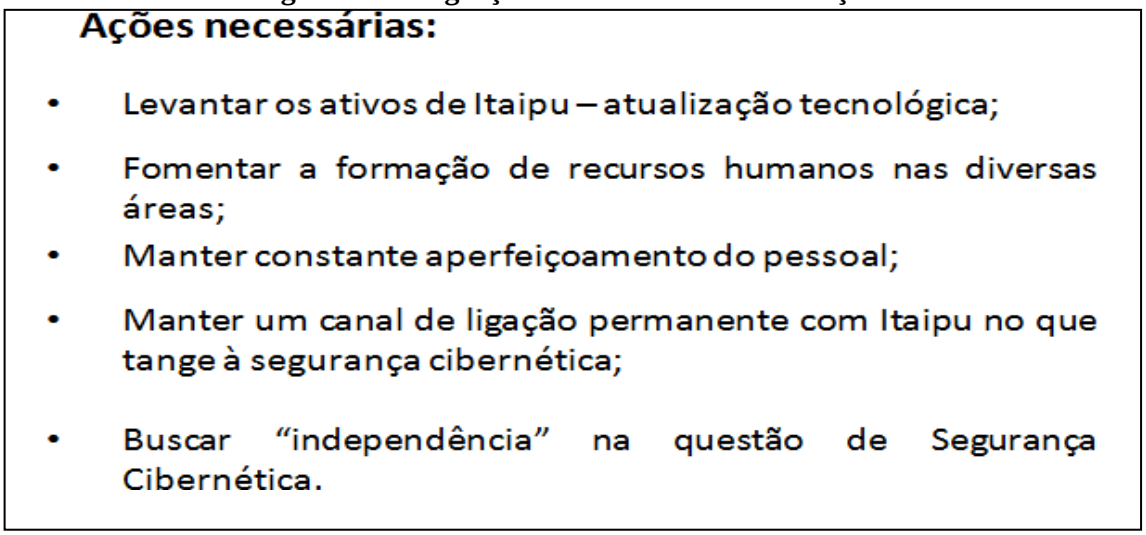
Figura 8 - Integração dos Centros de Simulação

Fonte: o autor, 2019.

3. Conclusões

Como conclusão, entende-se que as seguintes ações são necessárias para a consecução do projeto que o Exército Brasileiro desenvolve em parceria com a usina de Itaipu:

Figura 9 - Integração dos Centros de Simulação



Fonte: o autor, 2019.

Muito obrigado!

STRATEGIC PERSPECTIVES ON CYBERDEFENSE

Joe Devanny*

1. Introduction

They work closely in collaboration with the National Technical Authority (NTA) but it is not something and I will overemphasize. The fact that the patchwork quilt of responsibility is equally as complicated as it is eerie, everyone is working closely with each other and the manager of this coordination has been the Cabinet Office during the last 10 years.

We've gone through three iterations of all cybersecurity strategy in the UK. If you look at the years in Congress: one in 2009, the second one in 2011 that corrected what was wrong with the 2009 one, and five years later the 2016 strategy. Were explicitly produced to be King's College London to work for a five-year cycle the 2009 strategy wasn't necessarily designed for the time period, but the crucial piece of information you need to understand is that there is a strange lack of synchronicity because in 2010 there was an election and the government that had been in power for 13 years produced the country's first national cyber security strategy in 2009.

2. Development

That government lost that election and the incoming government which was a coalition government between a conservative and a liberal party decided that national security was one of the major areas they wanted to reshape. So in 2010 the government's approach was to introduce a five-year cycle of national security strategy which was aligned with a strategic defense and security review. So that explains some of the ways and means.

They were meant to all coexist with one another across a five-year lease cycle, but from that national security strategy there were offshoots of other strategies and the cyber security strategy was one of the first of those produced the following year.

User behavior and logical innovation run far ahead of bureaucracies' ability to produce strategy, policy, and implementation. In this way there's a constant sense of catch up where you produce a strategy that you know is outdated on the day that it's produced.

---

* PhD in Political Theory and Lecturer in the Departmenmte of Wars Studies at the King's College London (KCL).

While arguably it's already outdated on the day that it's produced it also can't possibly hope to represent future proof and, you know, it also can't hope to keep pace with innovation in all sectors.

The third factor, that once again is evident in many of the strategic documents, is government's recognition that it competes with the private sector for expertise. So there's a sense in government that it finds it very difficult to recruit, as well as to retain, skilled cyber-security professionals.

There are a number of different policies and initiatives that I'll talk about later where government tries to address this problem of recruitment and retention of experts. A sort of subsidiary of this genuine problem is that government recognizes that it needs to collaborate much more with the private sector. The fact that a lot of the necessary expertise is in the private sector it is only logical to use it knowing that a lot of the cyber defense innovations of the last five years have actually been built by and operated by the private sector.

I'll talk a bit later about the active cyber defense program and one major plank of that literally is built and operated by a private sector company. I've mentioned already the fact that there is this untidy landscape of institutional actors which you know potentially isn't as bad a problem as it looks but that might be a complacente British response to it.

There may be a case for a better coherence and streamlining of responsibilities not least of which because there has been a competition for control of certain aspects of cyberstrategy. There's an interesting debate that has seeped out into the newspapers to some extent between the Ministry of Defense and **Government Communications Headquarters**, commonly known as **GCHQ**, referencingt the ownership of the offensive cyber program which in itself is a collaborative program.

I'll talk about that a little later, but the overlapping on tidiness of the institutional landscape can cause problems and friction in the way that government implements the strategic agenda. Another thing, the penultimate thing is that the strategic approach, whilst there are lots of things in common in the three national strategies, has changed and especially the approach which changed between 2011 and 2016.

I'll also talk about it a little later, but there was a very public recognition by the government that the 2011 strategy had not been as effective as it should have been. As a result of that the government needed to become what was actually missing in the cybersecurity strategy, that is to be better comuunicator with the public and the private sector.

Furthermore to improve the awareness, understanding, and capability in cybersecurity so that the 2009 strategy has this "very 2009 vintage graphic" that they have clearly created in whatever iteration of word that was current then but it reflects something that again is a pretty useful and fairly consistent typology.

For understanding the British approach to cybersecurity you need to know there are objectives to reduce risk in cyberspace to exploit opportunities which in essence is a leaked reference to offensive cyber capabilities, cyber espionage operations, and, lastly, the knowledge capabilities and decision-making which is the education and development strand that's current throughout.

In all interations of the strategy one of the main things is in a relatively short document. The 2009 documents are only about 30 pages and if you strip out all the blank pages it's more like 20 pages but one thing it accomplished was to try to scope out all of the different strands of government work in cyberspace. Police and legislative sort of regulatory framework the cultural awareness issue skills and education which obviously brings together roles and responsibilities.

I have stated it hasn't quite been decided conclusively even now in international engagement if diplomacy should be more in the military space or the intelligence space exploitation and down in the bottom left what you won't be able to see is the technology in developing the research and development for cyber expertise. These are important details in that strategy but it was an exercise in King College London the strategic challenge that it did accomplish some reforms of the institutional landscape.

I said before they were mainly focused in the Cabinet Office at the center of government so it recognized that there needed to be more coordination of policy thinking and strategic thinking about cybersecurity. Thus as an incremental step forward they created an office for cybersecurity which was very quickly renamed the Office for Cybersecurity and Information Assurance to expressly provide that coordination of policy and strategy.

The other institutional reform was creation of the Office for Cyberoperations which and was essentially a creature of GCHQ, based in Chapman, west of London. So there's sort of two institutional mechanisms that took about a year to create as an EIN strategy but neither of those I believe were fully operational until the second quarter of 2010 which was only two months before the election.

So you can see one of the reasons why the manifestations of the 2009 strategy were actually replaced by what became the 2011 framework is that there is also a

recognition of something called the Computer Electronic Security, a group much more commonly known in its lifetime as CES.

If you go by its full name people wouldn't necessarily have understood what you were talking about whereas CESG everybody understood as the National Technical Authority for Information Assurance (IA). So they are still under a different name as part of GCHQ. The National Technical Authority is part of the British domestic infrasturcture. They have a foreign affairs that falls under the Intelligence and Security Agencies and that remains the case until today.

I talked about the sort of broader strategic trend in British government. It's been broadly well received, but there have been some criticisms of the quality of strategic deliberation so a former chief of the Defense Staff who sat on the National Security Council reflected this in written documents and skeptically spoke about the quality of strategic thinking in British government.

This means talking about strategy and geopolitical issues and actually thinking strategically and he has mostly criticized some geopolitical decisions. It's a broader question about the ethical Security Council process with the National Security Council being the body that approves strategic documents like the cybersecurity strategy. It is not the case that there's uniform acceptance and positivity about the strategic turn in British government.

Another sort of slightly more nuanced judgment from a former director of GCHQ who is here talking about the step from the 2011 to the 2016 strategy, as a reflective former practitioner. The landscape was quite untidy like.

The first objective is more domestic and/or enforcement orientated. It's about combating cyber crime usually in the document like cyberterrorism is very quickly mentioned thereafter.

Again that is sort of a position of protection of networks, but also resilience of networks and Society; the third objective. I'm passing one about public confidence and ability to operate in cyberspace and again appears this cross-cutting recurring theme about improving capability, knowledge, research, and development.

Even though this is a product of a different government, a coalition government that had very strong critical views about the performance of the previous government in the wider security space, more consistency and more similarities between those strategic approaches exist now and the coalition government did a number of things in the cyberspace both in narrow security and a broader sort of defensive terms.

The first thing that's worth mentioning is that the 2010 National Security Strategy for the first time made cyber a Tier one national in a more collegial and regular transparent way. A government criticism that had been leveled on Tony Blair especially during the period leading up to the Iraq war. One of the subcommittees of that NSC was a cyber subcommittee that had a larger cast of senior practitioners.

Again they are sort of a symbol of government taking cyber more seriously. In 2011 there was the new strategy and one of the headline-grabbing pieces of that was a national security program. They initially capitalized a little over 600 million and in that life cycle of five years it went up to 860 million. A fairly significant investment, but you know relatively-speaking still quite modest over a five year period across the whole government.

It wasn't the totality of government spent on cyber security. It was a specific program: all of the main departmental functions.

If you add them up, you can more or less double that figure but probably more than double was another thing they created in the more defensive space and that was Joint Force Command. The imperative to create was cyber, but cyber was one of the examples of ways in which the government felt defense would benefit from more coordination between the three services.

Things like surveillance intelligence shared functions, but cyber is one of the most salient shared functions that Joint Force Command has responsibility for. The chief of the Defense Intelligence Service has the personal ownership of the cyber part of that program that has taken several years to set up; the national offensive sniper program which again in military terms functions as part of Joint Force Command. It is an explicit collaboration between GCHQ and the military. Historically we will talk about it a little later.

Cyber offensive has been more a function of intelligence agencies than it has the military so GCHQ has certainly for over a decade, possibly for 20 years, had the authority to conduct offensive cyber operations.

If approved in the usual ministerial way whereas it's been a slower evolving process, the military operates in another institutional innovation which is the fourth bullet down. That is the creation in 2013 of something called the Center for Cyber Assessment, which was intended to provide strategic assessment and also strategic assessment across departments.

The Joint Intelligence Organization the Assessment Staff was deliberately created in the image of a body that existed about 10 years prior, called the Joint Terrorism

Analysis Center (JTAC), that was created to deal with terrorism in the 2000s. This because they represented the previous cross departmental strategic assessment. They didn't have the capacity or the expertise to be able to deal with terrorism as a strategic threat. They created JTAC and the similar sort of recognition or feeling in 2013 was that there was a need for a central strategic body, a generalist body, with the capability to deal with cyber on the street basis thus the Center for Cyber Assessment was created in 2013. Another artifact of that period to deal with the cyber skills gap in government and specifically in the military was the creation reserve.

It's reasonable to infer that the cyber reserve is a small percentage of the total military reserve. Very quickly to conclude on that coalition government, another King's College London in 2014 was the National Computer Emergency Response team which was responsible for dealing with threats to government networks. Again something that was housed in the Cabinet Office within the wider national security Secretariat and then lastly in 2015.

The coalition government dissolved due to another election in 2015 and the Conservatives won outright. From 2015 until today there has been a majority Conservative government but not a majority by a large margin. The 2015 national karate strategy produced by the Conservative government basically repeated the tier, one designation of cyber as a treaty. It is continuing that sort of symbolic importance of cyber as a strategic threat.

It announced that there would be the creation of a national cybersecurity center which to some extent is more evolutionary because it was a way of sweeping up lots of different functions done by several different organizations. The UK had only created it the previous year and had barely been set up by the time that national security strategy was produced in 2015.

I was immediately swept into this newly created organization called the National Cybersecurity Center. The largest percentage of the National Cybersecurity Center came from the National Technical Authority. At the beginning mostly all of the same people but under a different organizational structure and a new chief executive. A lot of machinery of government changes in the wider security space, but especially in the cybersecurity space over the last 10 years and obviously it takes time.

That whole budget went into central coordination policymaking which is quite a large overhead, This line is a product that was produced by GCHQ during the period of the coalition government and it was called 10 steps to cybersecurity. It's an example, I

mean a very ad hoc one, of the less than fair cybersecurity approach adopted by the government. This is an aide memoire for busy corporate executives to tell them in a very visual graphic way.

How they should design their organization's approach to cybersecurity?

How they should respond to increases of changing work patterns, people increasingly working from home, or using mobile devices?

What kind of security protocols if any are in place for that sharing of personnel incident management without a lot of detail?

An effortt in trying to sensitize corporate executives to think more seriously about cybersecurity. Now, obviously I did more than that but this is an example of one of the reasons why the 2016 strategy felt that they hadn't been active enough in changing people's atitudes, being more visible, and more interventionist in changing the culture of cybersecurity.

This is just a slide showing some other public information campaigns about cybersecurity.

Another institutional actor in that space was the Center for the Protection of National Infrastructure (CPNI) that helps with all the needs for critical infrastructure run out of the cabinet office. With a strong domestic security background, they were responsible for cybersecurity in critical national infrastructure until 2016 and the creation of the national cybersecurity center which took on the cyber component that they still worked closely with. The CPNI still exists to provide physical security and personnel security advice for that secretary.

You can go to their website and click on these and see more information about the kinds of user-focused public awareness campaigns, each of which are a part of the public side of the activities of these organizations. This brings us more or less up to date, at least for another year, which is the final year of the five-year lifespan of the -2016 strategy. It was quite a self-critical strategy.

I have put up here just excerpts quoted from the strategy where they reflect on what went wrong in the previous and what the promotion of cyber hygiene hasn't produced. We need to be more active and more interventionist. We need to have a bigger presence in the market to drive change.

They came up with a different way of conceptualizing the problem. They thought about what they had just read and they came up with three strap lines, so as to defend, deter, and develop the strategy. There is sort of a trend towards strategic inflation over

time in 2016. That strategy is about 80 or 90 pages long compared to the 25 - 30 pages in 2009.

Here, they say more things. They don't necessarily give you a greater depth of strategic insight. It's still a similar kind of vehicle as the 2009 or 2011 documents. They are about communicating with the public, communicating with allies and also communicating with adversaries.

You know that the crown jewels state secrets in these documents because they are intended to be unclassified documents. You have just the brief thumbnail definitions of each of those strap lines. Defense is obviously about defending networks. Deterrence about using all forms of all instruments of national power, not necessarily cyber and not confined only cyber, to deter adversaries whether state or non-state actors.

Then there is the education strand in 2009 and 2011. There is this consistency of strategic development even if the pace, change, and level of intervention has changed with the strategies. It's worth saying that although the government has changed; we are with on our fourth prime minister since 2010!

The people who work professionally in cybersecurity have changed a lot less than those in top leadership. They have perhaps changed almost that much but at the core you know people who were doing the work on this Aylin implementation and development are pretty much the same since 2016 until last week, because I can't comment on what Boris Johnson's cybersecurity strategy might or might not be.

I suspect if you asked him he couldn't comment either. I mean it will take some time for this current government to develop its strategy, but I would expect there to be more continuity than change because once again, like on the official side, the cast of characters is the same. The 2016 strategy recapitalized and reset the five-year cycle of the national cybersecurity program so it just about doubled.

I mean they talk about two different figures: 1.9 billion is a larger figure while 1.3 billion is the one that people talk about more. It's the same sum of money but it's just channeled in different ways and forms. I said earlier 1.3 billion or 1.9 billion is not the totality of government spending on cybersecurity. When you add it up that's in excess of 3.2 billion, but the program dedicated to innovation and improving capabilities is 1.3 billion.

We'll talk a little bit later about what they've actually done with that program but the biggest institutional innovation was the National Cybersecurity Center which does all of the same things as the organizations that it folded within itself.

It does it in a much more visible way, a much more energetic way, and also with a lot more prestige behind it.

It as probably much more visible on some of the slides.

The background to this slide is the headquarters of the National Cybersecurity Center which is a very prestigious building. I say skyscraper in Central London terms. It's not a big building, but it's an impressive looking building and it's very different from the traditional or classical or government offices that government departments are usually housed in at the center of London. This was a deliberate decision. A decision that was very expensive in terms of the commercial rent for those offices. It's not a government building and the decision was that they needed to change the image of cybersecurity as it reached out to government and from government to the private sector.

They needed an organizational approach, a branding, and a headquarters that looked like the sort of thing you would see in the private sector. The decision about where to house the cybersecurity center had that image in mind. I'm just quickly running through some of the things to bring us up to date.

I mentioned a few slides ago that the National Cybersecurity Center is now the indisputable National Technical Authority for cybersecurity but it doesn't control the cyber skill, and I stress cybersecurity skill strategy, produced by the Department for Digital, Culture, Media & Sport (DCMS).

That was in 2018, just last year, and there are a number of other initiatives that are part of the National Cybersecurity Strategy but are delivered through DCMS. One of the initiatives to improve the professionalization of cybersecurity in the UK is to create more clear professional pathways for people who are wanting to pursue careers in cybersecurity.

Not just in the usual way from schools although there's a lot of work in schools .but also in education in terms of funding student scholarships, bursaries, and apprenticeships funding PhDs. I'll talk about that in a moment. They're also trying to create some professional texture in a more interventionist way rather than just leaving it up to the market to work out on its own. This is to provide some government direction as to how the profession in cybersecurity develops. These are called the side or body of knowledge which you can navigate on their website and find out.

They have contracted in the main academics some practitioners to produce canonical statements of all of the core components of knowledge that you would need if

you wanted to pursue a career in cybersecurity and obviously this will need to be constantly updated.

A component of the program elaborated in 2016 is the active cyber defense program that can mean something slightly different if people talk about active defense. Sometimes people mean "hacking back" and the active defense cyber defense program in the UK is not "hacking back". It's about automating and increasing the scale and speed of things that were previously done on a manual basis.

It doesn't involve hacking into adversaries networks and to complete the flow there has been a number of government changes and also further strategies and sub-strategies movement in the last 12 months. One of those is the cyber security export strategy which is a very short document that's more of a statement of intent by the department for international trade which is effectively trying to demonstrate or persuade the security sector in the UK.

The government will actively help make business deals with foreign customers. There's a designated cyber security trade ambassador. I don't mean ambassador rank but a diplomat in UK missions around the world and a lot of countries whose job, or a large part of whose job, is to help British cybersecurity companies make business deals in foreign markets. It's na indication of an aspiration to have a comprehensive national approach to all aspects of the cybersecurity problem.

This is a good short sort of info graphic depiction of the UK's active cyber defense program that has been in operation for two years. In fact the NCSC released a 2018 report then apologized for releasing their 2018 report in July of 2019 but they said it took them that long to compare the data year-to-year. It could be more robust, but this is a good graphic depiction because it shows a number of different programs that are running the relationship between the government and private sector.

A number of these are either information sharing partnerships with the private sector for cybersecurity threats like the cyber intelligence sharing partnership while others, like trying to find the take down a notification servisse, in the bottom left is built and operated by a private sector company. The government set out the terms of reference that ran a commissioning process and that is owned and operated by a private company.

Some of the examples of things that the active cyber defense program does is it has an automated take down servisse; the one that I just mentioned. To give you one example of what it did in its first year: the UK´s share of visible global phishing attacks was halved.

I think 140,000 of those in the first year of the active defense program and it took it down from above 5%, the UK's global share of phishing attacks. Another sort of interesting indication is a kind of correlation causation that is not the same thing, but they are tentatively saying that it's an indication of the success of the program.

In 2017 they took down over 200,000 of 220,000 sites hosting malware in the UK. The take down is a legally prescriptive service. It's not a service that is done automatically by government to identify a site hosted on a UK IP address that contains malware. They send a polite letter of notification to the owner of the IP address and suggest politely that they might want to remove that website. It is not a legal letter and not legal proceedings.

If you look at the most recent report they generally have to make good take up. Just in the last year they have noticed that one of the major international web hosting sites that hosts a significant percentage of all web traffic also hosts proportionately infected malware as well. Things have actually gotten worse in responding to that approach.

I'm not putting this up as a paradigm for best practice that will inevitably lead to an improvement in the cyber hygiene of the national cyber space because it constantly has to be reiterated. You can see that in the subsequent year 2018 they had to take down fewer sites. They were related to about a third of the IP addresses corresponding to about half the number of individual unique campaigns.

You can say either they've had a significant effect at reducing the total amount of cyber active cyber crime activity or in a semi-joking manner you can use the NCS technical director's comments on the subject. When asked what his primary objective was with the active cyber defense program and he said: "Well, look it's not my responsibility to eradicate cyber crime. It's just to send it to France." The idea being that cyber security is a competitive enterprise.

You can do as a country to improve your own national cyber security and if you make it harder for criminals to operate in your own national cyber space, they'll just go somewhere else where they have worse cyber security. You know it there's that sort of semi-joking about the national rivalry between the UK and France, it's an indication of how one government's advances in cybersecurity should spur other governments to improve their cybersecurity as well. There's a virtuous circle in theory and then cyber criminals will find it.

It very difficult to operate anywhere. Another indication of the success of the program is that her Majesty's Revenue and Customs, which is the British tax collection agency, was the 16th most phished website in the whole world.

Cyber criminals thought a couple of years ago, you know British people do a lot of their taxes online and they're very rich so let's try to steal credentials, commit fraud, and take a lot of money from British citizens. In the world it is now pretty high after just two years of operation of the active cyber defence program. It's now the 146th most phished site among the top 200 in the world. That´s still quite a lot but it's a lot better. It's one of those rank orders where the higher the number the better your cybersecurity.

In CSC they are being moderately pleased at the results of those strands of the active cyber defense program. I should say that the active cyber defence program is only operative on government public sector networks. The idea was to test out a number of these techniques on government-owned networks rather than release them into the wild in the private sector and for all citizens because some of the strands raised some issues about privacy and about the balance between security and liberty in particular.

The protective DNS program is effectively kind of a firewall on top of government networks so NCSE or ministers made a judgement after a submission from NCS see that it wasn't enough to educate users not to click on dodgy websites. If they were a government employee using a government machine and a government network they would just shut down their ability to access those sites and they've shut down a lot.

I mean access to something like 11,000 websites every month. Thus significantly reducing the threat posed by those websites to users on government infrastructure because government users can't navigate to them. Obviously it would raise implications for liberty if you rolled out nationally something akin to the Chinese approach to cybersecurity or to control digital information.

We are not there yet but it is an interesting public debate to be had about the role of government intervening at that level of user choice. Lastly add web check is a service where NCSC monitor the latest security threats. In the beginning they are just an advisory service.

They have no authority to force the system administrators for different agencies and departments to attach their networks but this is an automated system where they fire out updates to all of those relevant people across the public sector. They have access to the latest information about what needs to be done on the networks. It's not a fully interventionist strategy but it's somewhere in the middle between fair and taking central control. It's a way of using automation to make it slightly easier to protect government networks.

In the last section, I going to talk about cyber deterrence and offensive cyber. This graphic is from a British newspaper report describing British government thinking about offensive cyber which obviously was aimed at Russian hot face Vladimir Putin and blew down the image that was at the GCHQ headquarters in the UK.

I'm going to play a short video of a speech earlier this year by a man who at the time was the foreign secretary. He has since subsequently been sacked, but not because of this speech, but because he tried and failed to become the prime minister. Today's tools are different from those of the Cold War and our responses must be different to the British government.

A starting point is that we must impose a price on malicious cyber activity including interference and elections sufficient to determine or Italian States. We won't always react identically to every individual instance and a cyber attack will not necessarily encounter a cyber response.

Instead our approach to cyber deterrence has four principles. Firstly, we will always seek to discover which state or other actor was behind any maligned cyber activity by overcoming any efforts to conceal their tracks. Secondly, we will respond in ways that could include naming and shaming the perpetrator in public. In concert with our allies we will expose not only who carried out the action but as far as possible reveal how it was done, thereby helping the cybersecurity industry develop protective measures. Thirdly, we will aim to prosecute those who conduct cyber crime demonstrating they are not above the law. Fourthly, and finally, with open eyes we will consider further steps consistent with international law to make sure we don't just manage current cyber attacks but deter future ones as well now.

One of the most powerful tools is the sunlight of transparency that the British government has right. The public attribution even just two or three years ago the UK was much more allergic to making public attribution especially of state actors behind various cyber threats.

I think in part that was a reflection of the intelligence culture where this type of cyber expertise came from that there is this feeling that the more you put out into the public domain the more your adversaries will be able to infer about your own capabilities.

Actually you do not want to tell people that you know who was responsible because that will start to make people think about how you know that, what are the different techniques or national technical means used, and related matters. You need to make that assessment increasingly especially in the cases regarding Russia and China.

The UK has started to be much more public about attributing major attacks to state actors and as possible again consistent with a wider diplomatic strategy. It's not just the UK making that public attribution. It's all of their allies as well. It has the broader force of the international community thirdly. You know again the US and the UK approaches are in synchronization here where possible and often it's not possible initiating criminal proceedings against the actors who are responsible for those cyber attacks.

Now, their state actors are more likely to be protected by the state that they are working for but there have been some cases of people being apprehended especially if they are in a third country.

Fourthly diplomatic is economic sanctions or sanctioning. This is the idea of cross-domain deterrence that Jeremy Hunt said in his speech it won't always be a cyber response to a cyber attack. We have a number of different instruments of national power and we'll use whatever single one or combination of instruments that we think is necessary to achieve that deterrent effect or retributive punishment effect.

Lastly, I can't remember the euphemism he used but it's something consistent with international law by which he meant offensive cyber which is a component of the UK suite of deterrent measures.

Another more recent defense staff person said very recently in testimony to Parliament that essentially cyber deterrence does exist, but it's relative immature as a discipline and as a doctrine we're learning. The people shouldn't just assume that cyber deterrence is purely a function of cyber capabilities and he said that he's making the conventional point or conventional and nuclear point that all this is just a quick line about the international normalization of talking more about offensive cybernational capability.

I think John Bolton's moustache is very striking so since he's the national security adviser there's been definitely a greater sense of urgency. In the Washington Post and The New York Times we read about President Trump's administration replacing Obama's administration. It is still classified but unsurprisingly it has been reported in the usual places that it has a bigger risk appetite, and it is also that they are increasingly talking more openly and more often about their offensive cyber capability which is unsurprising if you wanted to have a deterrent effect on people. People are going to talk more about their offensive cyber capabilities as a classic form of SIC.

What they are doing is not surprising; there are plenty of instances. The GCHQ is instrumental in developing and delivering that ability for this.

Actually earlier this year the British defense secretary was sacked because the Prime Minister and cabinet secretary felt he was responsible for a leak of information to a newspaper about Huawei and Chinese investment in UK critical infrastructure. People have been sacked for leaking to the newspapers, but it's pretty uncommon, but this is a separate story from earlier this year.

I don't know the story exactly from late last year but in October the UK Ministry of Defense had been wargaming cyber attacks on Moscow. It is an extraordinary story that I encourage you to look at. It's a short one but the gist of the story is the highly classified planning meeting, that's not so highly classified that the people were telling the Times about them.

They were meeting once a week and they concluded that cyber weapons, sort of newspaper speak for offensive cyber, would give Britain the best chance of deterring a Russian attack on the West.

You know, very vague, but they go on to clarify because the UK no longer has access to small battlefield nuclear weapons. It's not a very precise story but they have cited anonymous sources.

If Russia sank our aircraft carrier with a nuclear-tipped torpedo, how would we respond. You can go on the offensive. You can touch the lights in Moscow to tell them that they are doing the right things which is like a fairly immature approach to cyber sick to grow its number from five hundred to two thousand personnel.

It is a significant increase in the manpower capability and at the same time last year the defense cyber school was created. It is another indication that the three services the Ministry of Defense are becoming more active in the cyber sphere and I would say in the medium term that the likely end point is just a gradual evolution in the joint cyber force that the military will continue to take more control over. The balance between them and GCHQ will shift more in the defense direction but we won't as a cyber command because just the numbers don't really justify the development of separate capability.

You would imagine over time that the offense of cyber force will get bigger, but it's starting from a very small base line and here just very quickly you have two former senior generals former CVS and form of VCDs talking about some short comings about the joint force approach.

On the one hand the joint force approach is a relatively recent phenomenon in innovation that has a lot of support behind it but they have some skepticism or uncertainty about how the single services are important.

He's not sure that the single services are necessarily sending their best people to be part of Joint Forces Command. Nick Cotton is saying that he has heard people refer to Joints Forces Command as a purple skip by which he means a sort of a joint service institution where if you're not really sure where to stick a capability give. It's to the Joint Forces Command.

It's a fundamentally good idea but it has to be treated as such. It has to be taken seriously, buy into it to me and this is in ship but to buy GCHQ in the past ten years. Will we start to see that change in time? I think we should but it probably won't be fast.

Just going to quickly show you some of the education innovations that have happened over the last five or six years. This is just the last recurring strand of the cybersecurity strategy. It's not just about changing the institutional coordination and the offensive capabilities but it's about changing the cyber skills landscape.

This is just a short promotional video that was produced recently for one of their flagship educational programs targeting teenagers and school children in high school. This is a world where technology is everywhere. It's smooth running trains and safe flight paths for planes. It's power to the grid and power to the people and it's where hashtag to words can start a movement, where two lonely hearts can meet, technology means new troubles fast, what goods travel to Boston, language translation for film and music creation, and if the life-or-death surgery goes without a hitch. Technology is everything and it means everything. It's means protecting it at every stage.

Every walk of life will come together to safeguard our digital planet because this protection touches lives in a million different ways. We know that cybersecurity is our first line of defense. This is being a modern citizen. This is finding out there is a defense component to that again targeting children.

I'm going to play here a short clip from the most recent Conservative Party Conference. This gentleman was actually the defense secretary who was subsequently sacked for leaking confidential information but he's here talking about a defense program for cadets, all children in the military.

This will be a chance for all of us to come together to see everything and how young people gain. We teach the cadets new skills that are vital for succeeding in today's world where being savvy online and protecting against cyber attacks are essential.

I'm pleased to launch a new cyber security training program for our cadets. This program has been designed with GCHQ and at the National Cyber Security center 2.000 cadets a year will be trained in cyber security.

It was a sufficiently salient issue that he made one of his signature announcements at the party conference that was for 2.000 children a year and there were about 40.000 cadets. It's a small proportion of the cadets and it cost about a million pounds a year to fund that but it's an indication of the integrated government response to improving the cyber skills landscape. So Cyber First is the wider program targeting all school children in the UK not just cadets. They run a number of programs in different age groups including national competitions. There's one that is the cyber first girls' competition to improve diversity in the cyber security field and finally the government is also looking at the areas that you'd expect them more traditionally to be looking at in education.

Sponsoring degree programs and bursaries for people to take cyber relevant degrees but also degree apprenticeships where you are actually on a program where you are working and the government gives you work experience at the same time. You are being paid to earn your cybersecurity degree. There are a number of different programs, at this sort of undergraduate level and then at the postgraduate level they're funding.

I think they're about 28 doctorates that have been funded already on that program. The ambition is to make that 150 by 2024 so they have to get a move on or they will probably miss the target but it is an indication of intention.

They have also funded 14 centers of excellence and 4 university research institutes in cybersecurity so there's a significant momentum behind it institutionally as a program to improve cybersecurity capability outside of government and further improve the pipeline of people going into the profession.

Lastly, I just want to raise this issue of oversight. In the last tem years there have been a lot of activities in the cyber area, security cyber defense, offensive cyber and the like. I spoke about strategy in the UK as an oversight of cyber is vulcanized quite segmented Joint Committee on the national security strategy which is a joint house of parliament committees that investigates the whole of national strategy but they've been very interested in cybersecurity as an issue.

The Defense Select Committee actually has no remit to investigate operations so no cyber options can be investigated by the parliamentary defense committee. They can have a look at a wider strategy and budget and things like that but in parliamentary scrutiny of defense issues and security issues it doesn't have a huge amount of capacity behind. It is a potential area for future growth but I wouldn't say that there's a significant interest in Parliament in taking on more abilities.

If you compare UK oversight with US oversight the US congress members and senators have a lot more powers off a much bigger budget to be able to scrutinize government activity in this area. If it does have a remit to investigate operations it is the Intelligence and Security Committee of Parliament which is a very special committee. It's not appointed in the same way the other committees political parties elect their members. To serve on the Intelligence and Security Committee the members are appointed by the Prime Minister because it has access to classified material in a way that the other committees do not.

3. Conclusion

I try to convey that it has been a slow evolution of policy and strategy in the UK but they have been doing some interesting things. They have had, broadly speaking, the same strategic understanding of the issues. The pace and scale and acceleration of the quality of the intervention of government in the field has changed especially in the last five years and I'd expect that to continue unless something fundamentally surprising happens under the Boris Johnson government, which is possible.

I'd expect that same pace and intensity of government intervention to continue so that there are open questions about what the next cybersecurity strategy will look like whether there'll be another five-year program for cybersecurity or the offensive cyber program or whether that becomes more mainstreamed within the government budgets of the relevant agencies and actors. Broadly-speaking I would say there will probably be more continuity and change because although it's a new issue in terms of capability. The way the government has approached it has been nearly as they would approach any other security issue. The same sort of strategic and policy responses.

Thank you very much for listening. I very much welcome questions afterwards.

Thank you again!


CICLO DE
ESTUDOS ESTRATÉGICOS

Agência Brasileira do ISBN
ISBN 978-85-64844-05-6