UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DIRETORIA DE PESQUISA E PÓS-GRADUAÇÃO
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZAÇÃO EM REDES DE COMPUTADORES E TELEINFORMÁTICA

ALEXANDRE LIRIA BENELLI

ANÁLISE DO CIBERTERRORISMO E CIBERSEGURANÇA

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA
2018

ALEXANDRE LIRIA BENELLI

ANÁLISE DO CIBERTERRORISMO E CIBERSEGURANÇA

Monografia de Especialização, apresentada ao Curso de Especialização em Redes de Computadores e Teleinformática, do Departamento Acadêmico de Eletrônica – DAELN, da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. Esp. Douglas Eduardo Basso

CURITIBA
2018

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Câmpus Curitiba

Diretoria de Pesquisa e Pós-Graduação
Departamento Acadêmico de Eletrônica
Curso de Especialização em Redes de Computadores e Teleinformática

TERMO DE APROVAÇÃO

ANÁLISE DO CIBERTERRORISMO E CIBERSEGURANÇA

por

ALEXANDRE LIRIA BENELLI

Esta monografia foi apresentada em 30 de novembro de 2018 como requisito parcial para a obtenção do título de Especialista em Redes de Computadores e Teleinformática. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. Esp. Douglas Eduardo Basso
Orientador

_____
Prof. Dr. Kleber Kendy Horikawa Nabas
Membro titular

_____
Prof. M.Sc. Omero Francisco Bertol
Membro titular

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

À minha família, pela compreensão em todos os meus momentos de ausência, para que eu sempre pudesse atingir um objetivo.

AGRADECIMENTOS

Ao professor Douglas Eduardo Basso por ter acreditado neste trabalho e conduzido com sabedoria ampla e objetiva, guiando-me até o final desta jornada.

Ao corpo docente do Curso de Especialização em Redes de Computadores e Teleinformática, do Departamento Acadêmico de Eletrônica (DAELN), da Universidade Tecnológica Federal do Paraná (UTFPR), pelos ensinamentos, profissionalismo e abnegação demonstrados no decorrer do curso.

Aos meus pais, irmã, familiares e colegas de sala.

Às pessoas que sempre farão parte desta etapa da minha vida. O meu mais sincero obrigado.

*“*Na guerra, a **verdade** é a primeira vítima”.
Ésquilo

RESUMO

BENELLI, Alexandre Liria. **Análise do ciberterrorismo e cibersegurança**. 2018. 57 p. Monografia de Especialização em Redes de Computadores e Teleinformática, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

Com a expansão das redes de computadores, o que permitiu uma comunicação mais acelerada, rompeu fronteiras na disseminação das informações, seu uso para facilitar o cotidiano de grande parcela da população mundial, se aliaram a estas facilidades o uso do Estado em oferecer serviço para a população, ocorrendo uma grande desburocratização de serviços e facilitando o acesso do público a estes serviços. Esta popularização criou uma rede de coordenação dos países em alocar sistemas remotos, serviços e em alguns casos a própria estrutura governamental, com transmissão de dados sensíveis e operações financeiras. À medida que a popularização de acesso aumentou gradualmente no decorrer dos anos, aumentaram as formas de tentar corromper esta rede, sendo de maneira jocosa, como um desafio, para meios ilícitos e outras como ligadas a pequenos grupos, envolvendo apenas um ator, chegando nos dias de hoje o seu emprego de forma terrorista por grupos mais radicais e por países como uma forma de defesa e prevenção. Após incidentes que ocorreram em alguns lugares do mundo, ficou evidenciado que estas ações no mundo cibernético atingem de forma direta bens, serviços e até mesmo a soberania de países, elevando a maneira de enfrentamento e prevenção. Exemplos cotidianos de roubo de dados sensíveis, tentativa de acesso em banco de dados de estruturas governamentais e grandes corporações, expõem que um ataque ou uma interrupção de serviços bem sucedido pode ocasionar, onde o cidadão comum sempre será o mais lesado. Estas atividades entraram na pauta, como aqui no Brasil, em estratégias de defesa nacional, prevendo que as guerras no futuro sairão do que se conhece hoje como guerra convencional, aquela onde os embates ocorrem no plano físico, e sim passando a ocorrer no meio cibernético, com igual ou maior letalidade. Esta pesquisa bibliográfica apresenta um estudo sobre a perspectiva de ataques coordenados e assimétricos, sob a égide de uma ideologia, causa ou manifesto de um grupo autodenominado, que através da rede de computadores, lança um ataque que tenha como objetivo causar a instabilidade do tráfego de dados e seus serviços essenciais em uma nação ou continente, diferenciando de um ataque *hacker*, ciberativismo ou cibercrime. E analisar o posicionamento do Brasil neste contexto de esfera global.

Palavras-chave: Terrorismo. Brasil. Tráfego de Dados. Ciberterrorismo. Cibersegurança.

ABSTRACT

BENELLI, Alexandre Liria. **Cyberterrorism and cyber security analysis**. 2018. 57 p. Monografia de Especialização em Redes de Computadores e Teleinformática, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

With the expansion of computer networks, which allowed a more accelerated communication, broke boundaries in the dissemination of information, its use to facilitate the daily life of a large portion of the world population, allied to these facilities the use of the State in Provide service to the population, occurring a great debureaucratization of services and facilitating public access to these services. This popularization has created a network of coordinating countries in allocating remote systems, services and in some cases the government structure itself, with transmission of sensitive data and financial operations. As the popularization of access has gradually increased over the years, the ways of attempting to corrupt this network have increased, being in a playful manner, as a challenge, for illicit means and others as linked to small groups, involving only one actor, Today, its use in a terrorist manner by more radical groups and by countries as a form of defense and prevention. After incidents that occurred in some places of the world, it was evidenced that these actions in the cybernetic world directly affect goods, services and even the sovereignty of countries, raising the way of coping and prevention. Everyday examples of sensitive data theft, attempted access to a database of government structures and large corporations, exposes that a successful attack or interruption of services can cause, where the ordinary citizen will always be the most injured. These activities entered the agenda, as here in Brazil, in national defense strategies, predicting that the wars in the future will come out of what is known today as conventional warfare, the one where the clashes occur in the physical plane, but rather occurring in the midst cybernetic, with equal or greater lethality. This bibliographic research presents a study on the perspective of coordinated and asymmetric attacks, under the aegis of an ideology, cause or manifest of a self-styled group, which through the computer network, launches an attack that aims to Cause the instability of data traffic and its essential services in a nation or continent, differentiating from a hacker attack, cyber activism or cyber-crime and analyze the positioning of Brazil in this context of global sphere.

Keywords: Terrorism. Brazil. Data traffic. Cyberterrorism. Cybersecurity.

LISTA DE QUADROS

LISTA DE FIGURAS

LISTA DE SIGLAS

ABIN	Agência Brasileira de Inteligência
ADSL	*Assymetrical Digital Subscriber Line*
APF	Administração Pública federal
C^2	Comando e Controle
CDCiber	Centro de Defesa Cibernética
CF	Constituição Federal
CIA	Central de Inteligência Americana
CSIRT	Grupos de Resposta a Incidentes de Segurança em Computadores
CTIR Gov	Centro de Tratamento de Incidentes de Redes do Governo
DDoS	*Distributed Denial of Service*
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name System*
DSIC	Departamento de Segurança da Informação e Comunicações
EB	Exército Brasileiro
EMCFA	Estado-Maior Conjunto das Forças Armadas
END	Estratégia Nacional de Defesa
EU	União Europeia
EUA	Estados Unidos da América
FA	Forças Armadas
GSI	Gabinete de Segurança Institucional
IDCiber	Instituto de Defesa Cibernética
IP	*Internet Protocol*
LBDN	Livro Branco de Defesa Nacional
MC	Manual de Campanha
MD	Ministério da Defesa
NuENaDCiber	Núcleo da Escola Nacional de Defesa Cibernética
OSP	Órgãos de Segurança Pública

PR	Presidência da República
SISMC²	Sistema Militar de Comando e Controle
SSH	*Secure SHell*
TIC	Tecnologias da Informação e Comunicações
USA	*United States of America*
WEB	*World Wide Web*

SUMÁRIO

1 INTRODUÇÃO

A evolução das maneiras de comunicação que a acompanham a humanidade no decorrer dos séculos, facilitou a propagação de conhecimento e cultura, bem como diminuiu as distâncias entre povos de diferentes continentes, expandiu territórios. Além disso, é inegável que, por meio dessa evolução, a tecnologia envolvida nesses processos, se tornou acessível a grande parcela da população mundial, fazendo com que a humanidade se conectasse com o que hoje se denomina internet.

A sua acessibilidade trouxe grandes avanços na forma de comunicação e ofertas de produtos e serviços. Trouxe também uma forma menos dispendiosa para que governos e corporações agilizassem seus processos, tornando-os mais acessíveis e menos burocráticos, o que possibilita a economia de tempo e de gastos para o funcionamento estrutural e corporativo.

Paralelo a essa demanda de uso da internet, cresceu também a dependência de grandes corporações e principalmente de países na utilização da internet. Essa dependência é tanto do tráfego de dados sensíveis quanto do controle de subestações de energia, por exemplo, surgem usuários, dotados de conhecimento técnico com o objetivo de prejudicar este sistema. Uma parcela de usuários que começaram a penetrar e subtrair estas informações, bloqueando o funcionamento de páginas entre outros ilícitos, onde se institui o termo *hacker,* que é o usuário dotado de certo grau de conhecimento técnico que consegue manipular o tráfego de dados para diversos fins.

Nesse sentido, no final do século passado, após a intervenção americana no Iraque, houve um crescente número de grupos contrários a essa invasão, iniciando um ponto de inflexão entre países ocidentais e orientais: a disseminação de ideologias, o recrutamento de pessoas, assim como a instabilização de áreas sensíveis, como, por exemplo, usinas nucleares. O acesso de dados na área bélica se tornou uma espécie de ‘arma’ para interesses diversos, principalmente, escusos. E em decorrência do alinhamento ou apoio de nações, sob os mais diversos interesses, nasce o que se denomina terrorismo cibernético. Na contramão desse formato de terrorismo, surge também tudo que envolve a sua prevenção, logo, tudo que envolve a cibersegurança.

1.1 TEMA

Este trabalho analisa o terrorismo cibernético, bem como suas causas, seus atores e suas consequências. Ademais, analisa as formas utilizadas pelas nações para analisar e empregar medidas preventivas acerca deste assunto, em especial, como o Brasil interpreta a questão do terrorismo. Outrossim, este estudo apresenta casos específicos envolvendo o terrorismo cibernético.

Para tanto, foi necessário considerar a ampliação gradual do conceito de segurança para as nações, tendo em vista que é a condição que permite ao país: preservar sua soberania e integridade territorial, promover seus interesses nacionais livre de pressões ou ameaças, e garantir aos cidadãos o exercício de seus direitos e deveres constitucionais. Além disso, preservar a segurança requer medidas de largo espectro, as quais envolvem, além da defesa externa: a defesa civil, a segurança pública e as políticas econômica, social, educacional, científico-tecnológica, ambiental, de saúde, industrial (BRASIL, 2012). Por fim, este trabalho analisa a que ponto o terrorismo cibernético pode evoluir como arma para vencer um objetivo.

1.2 PROBLEMA

A Doutrina Militar de Defesa Cibernética, conhecida como MD31-M-O7, rege que “O Brasil, como nação soberana, necessita possuir capacidade para se contrapor as ameaças externas, de modo compatível com sua própria dimensão e suas aspirações político-estratégicas no cenário internacional” (BRASIL, 2014, p. 13), e ainda cita:

> Na atual conjuntura mundial, caracterizada por incerteza, mutabilidade e volatilidade das ameaças potenciais, bem como pela presença de novos atores não estatais nos possíveis cenários de conflito, a sociedade brasileira, em particular a expressão militar do Poder Nacional, deverá estar permanentemente preparada, considerando os atuais e futuros contenciosos internacionais. Para tal, medidas deverão ser adotadas de forma a capacitá-la a responder oportuna e adequadamente, antecipando os possíveis cenários adversos à Defesa Nacional. (BRASIL, 2014, p. 13).

O futuro amparo e diretrizes deste assunto são vinculados no projeto denominado Livro Verde, elaborado no ano de 2010, pelo Governo Federal, que deu subsídio para a confecção do projeto Livro Branco, que veio a se tornar a Estratégia

Nacional de Defesa (END) em 2012, que preconiza que para se opor a possíveis ataques cibernéticos, é essencial aperfeiçoar os dispositivos de segurança e adotar procedimentos que minimizem a vulnerabilidade dos sistemas que possuam suporte de tecnologia da informação e comunicação (TIC) ou permitam seu pronto restabelecimento (BRASIL, 2012).

Em conformidade com essa linha de pensamento, Basso (2015, p. 13) afirma que:

> Chama a atenção que o chamado espaço cibernético, não tem suas fronteiras ainda claramente definidas, impacta o dia a dia de todos os dirigentes governamentais, de empreendimentos privados e dos próprios cidadãos. Na nova conformação da Sociedade da Informação, vale destacar os seguintes fenômenos:
> - Elevada convergência tecnológica;
> - Aumento significativo de sistemas e redes de informação, bem como da interconexão e interdependência dos mesmos;
> - Aumento crescente e bastante substantivo de acesso à internet e das redes sociais;
> - Avanços das tecnologias de informação e comunicação;
> - Aumento das ameaças e das vulnerabilidades de segurança cibernética;
> - Ambientes complexos, com múltiplos atores, diversidade de interesses, e em constantes e rápidas mudanças.
>
> Neste contexto, as estratégias internacionais no tema apontam para o estabelecimento de parcerias e ações colaborativas efetivas entre países, que propicie a análise, a coordenação, e a integração dos conhecimentos, permitindo, além da correlação entre tais conhecimentos, o entendimento dos impactos que a convergência e a interdependência existentes, e ainda por vir, têm e terão no futuro.

1.3 OBJETIVOS

1.3.1 Objetivo Geral

Analisar o terrorismo, ciberterrorismo, suas motivações e a cibersegurança no cenário brasileiro.

1.3.2 Objetivos Específicos

Para atender ao objetivo geral neste trabalho de conclusão de curso os seguintes objetivos específicos serão abordados:

1. Compreender o significado das palavras ‘Terrorismo’ e ‘Cibernético’ em um breve histórico, bem como a definição mundial sobre grupos terroristas que utilizam a internet como forma de divulgação e recrutamento;
2. disponibilizar uma análise sobre o terrorismo cibernético e o futuro aperfeiçoamento do cenário preventivo no estado brasileiro;
3. apresentar a legislação pertinente e a forma de compreensão do estado brasileiro acerca do assunto;
4. demonstrar casos de terrorismo cibernético e seus atores;
5. analisar a forma de prevenção para o terrorismo cibernético.

1.4 JUSTIFICATIVA

O assunto ainda é pouco explorado no meio acadêmico, mesmo que sempre apareçam nos meios de comunicação situações de interferências em órgãos governamentais como invasão em sítios digitais, influência em resultados eleitorais, influências em resultados de concursos públicos etc. A tentativa de invadir sistemas públicos ou privados cresce dia a dia, pelo fato de grande parte da população seguir ideais que lhe convenham e o alinhamento da forma como alguns países são administrados e também exercem sua influência, exteriorizam-se por meio da internet atividades de cunho ideológico que nem sempre podem ser classificadas como terrorismo cibernético e sim como ciberativismo, ataque *hacker* entre outros.

1.5 METODOLOGIA

A metodologia utilizada é a de pesquisa bibliográfica, a qual foi realizada por meio de pesquisas em livros, manuais, teses e sítios eletrônicos de órgãos oficiais e técnicos especializados, para coleta de uma base para realizar uma explanação do atual cenário.

1.6 ESTRUTURA DO TRABALHO

Esta monografia de especialização está dividida em 5 (cinco) capítulos. No primeiro capítulo foi introduzido o assunto ema do trabalho e também foram

abordados a motivação e os objetivos geral e específicos da pesquisa, assim como a justificativa e a estrutura geral do trabalho.

No segundo capítulo: o tema **Terrorismo e Cibernética** são abordados de forma direta com a denominação corrente por autores ligados ao assunto e alguns órgãos de segurança. O tópico **Segurança da Informação** discorre sobre os pilares básicos e o valor que a informação possui.

A seguir, no terceiro capítulo: **Cibernética e seu significado**, meios utilizados para tentativa de invasão no meio cibernético pelo terrorismo. Encerrando este capítulo com estatísticas de ataques ocorridos no Brasil.

No quarto capítulo: **Legislação brasileira e órgãos de responsabilidade sobre Defesa Cibernética,** discute-se como o assunto é tratado a nível de segurança nacional, bem como sua homologação no território nacional, do ponto de vista conceitual, com **Análise de Casos,** tendo como base os ataques de características terroristas ocorridos na Estônia em 2007, Irã em 2010 e Brasil em 2003.

Por fim, nas **Considerações finais**, se apresenta as análises deste trabalho, assim como uma previsão do futuro deste assunto no âmbito nacional. Neste sentido, a análise se debruça sobre o que é terrorismo cibernético e o que isto representa atualmente em legislações brasileiras, no âmbito da cibersegurança, com enfoque aos meios que previnam este tipo de terrorismo e a possível identificação de seus atores.

2 TERRORISMO E CIBERNÉTICA

Este trabalho se inicia com a análise do cenário mundial, do qual o uso da internet para propagação de ideias e ideais se tornou mais crescente no início deste século, por grupos ou pessoas, que por intermédio da rede de computadores acelera o processo destas difusões, fazendo com que novos seguidores destas causas ingressem ou sejam difusores de causas ou atividades. Nestas filiações agregam-se em suas fileiras pessoas das mais variadas classes sociais e níveis intelectuais, utilizando seus conhecimentos em função da qual está sendo doutrinado. Nesta visualização o emprego dos meios oferecidos pela internet e o seu uso constante como ferramenta administrativa e operacional por corporações e nações, e face ao uso grupos coordenados utilizam dos mesmos meios para invadir os meios de transmissão de dados e assim propagar ou interferir no fluxo normal desta transmissão, causando grandes danos ao usuário final, neste caso a população.

Recentes ataques a rede mundial vem se tornando contumazes, seja de uma maneira escalonada como o corrido em 17 de maio de 2017 com o *crypto-ranzomware WannaCry*, ou entre países com o propósito de roubo de dados sensíveis ou interferências nas áreas bélicas e de inteligência. Em ambos cenários estas condutas são classificadas como ataques cibernéticos, roubo de dados, coleta de dados, ataques velados, etc. Sendo processados por disseminação de vírus ou por acesso remoto. O limiar do que seja um ataque *hacker* ou de que seja considerado um ataque terrorista é tênue. A definição de terrorismo é ampla e seu uso é histórico, citando Visacro (2009, p. 279):

> O terrorismo não é um fenômeno recente. A palavra faz lembrar dos radicais jacobinos e a institucionalização do “terror de Estado” praticado durante a revolução Francesa, por meio do Tribunal Revolucionário de Paris. Mas antes deles, diversos déspotas já haviam recorrido a esse método. O Czar Ivan IV, por exemplo, receber ao “terror” como alcunha, e séculos mais tarde esse ainda seria o principal recurso empregado por Stalin para dirigir a União Soviética. A Partir do século XIX, o terrorismo vem adquirindo uma importância crescente;.. Mikhail Bakunin, fundador do anarquismo russo, preconizava o uso do terror como ferramenta revolucionária. Em fevereiro de 1880, um atentado a bomba perpetrado pela organização Vontade do Povo vitimou o czar Alexandre II. Lênin e os bolcheviques, naturalmente, incorporaram o terrorismo a seu repertório sedicioso e, anos mais tarde, exportaram-no para todo o planeta, por intermédio dos agentes do *Kominter*. Outro atentado precipitou o início da Primeira Guerra Mundial, quando a Mão Negra (Organização Nacionalista Bósnia patrocinada pela Sérvia) assassinou o arquiduque Ferdinando da Áustria durante uma visita a Saravejo.

O terrorismo acelerou seus meios e a sua disseminação no cenário pós segunda guerra mundial, onde o mundo sofria uma polarização de ideias e a proliferação de grupos e suas ações envolviam principalmente reféns e visavam principalmente a publicidade de suas ações. Essas ações finais e o conjunto que advinham delas recebeu a definição de guerra irregular. Citando Von der Heydte (1990, s/p): “O terrorismo no combate subterrâneo é apenas um instrumento junto a outros. O terrorismo explica uma figura dirigente do movimento de guerrilhas (…) Ele deve somente ser usado como uma atividade intensificadora de apoio a outras ações”.

O Quadro 1 apresenta definições do que é considerado terrorismo por alguns órgãos de segurança mundial.

Quadro 1 – Definição de terrorismo para órgãos de segurança

Órgão	Definição
Departamento de Estado dos EUA	Violência premeditada e politicamente motivada perpetrada contra alvos não combatentes por grupos subnacionais ou agentes clandestinos, normalmente com a intenção de influenciar uma audiência.
Departamento de Defesa dos EUA	O Calculado uso da violência ou da ameaçam de sua utilização para inculcar medo, com a intenção de coagir ou intimidar governos ou sociedades, a fim de conseguir objetivos geralmente políticos, religiosos ou ideológicos.
Governo do Reino Unido	O uso da força ou sua ameaça com o objetivo de fazer avançar uma causa ou ação política, religiosa ou ideológica que envolva violência séria contra qualquer pessoa ou crie um risco sério para a saúde e segurança do povo ou de uma parcela do povo.
Agência Brasileira de Inteligência (ABIN)	Ato premeditado ou sua ameaça por motivação política e ou ideológica, visando atingir, influenciar ou coagir Estado e ou a sociedade, com emprego de violência. Entendem-se, especialmente por atos terroristas aqueles definidos nos instrumentos internacionais sobre a matéria, ratificados pelo estado Brasileiro. A Lei n° 13.260 (de 16 de março de 2016), disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13260.htm>, acesso em: 17 out. 2018 (BRASIL, 2016).

Fonte: Visacro (2009, p. 282).

2.1 DIFERENCIAÇÃO DE ATO TERRORISTA E GRUPO TERRORISTA

‘Ato terrorista’ e ‘Grupo Terrorista, conforme Brasil (2007, p. 15), são duas palavras distintas.

> Ato terrorista é qualquer expediente utilizado por pessoa, grupo de pessoas ou Estado que emprega força ou violência física ou psicológica, para infundir o medo generalizado entre a população e, com isso, atingir seus objetivos. Grupo terrorista é uma congregação de pessoas que emprega, preferencialmente, atos terroristas para alcançar um objetivo político ou ideológico.

2.2 PRINCIPAIS GRUPOS TERRORISTAS

O aumento de usuários da internet cresceu, assim como a diversidade de procura por serviços e informações disponibilizadas. Nesse sentido, essa ferramenta incrementou o *modus operandi* de grupos terroristas, os quais a utilizam para divulgação de atividades e recrutamento de novos integrantes. Percebe-se que em alguns desses sítios eletrônicos há a nítida contribuição de empresas especialistas em 'engenharia social' para recrutamento e exposição de ideais.

Por esse viés, a relevância acerca do tema levou a revista Forbes (2018) a listar os dez grupos terroristas mais ricos do mundo. De acordo com a revista, o grupo Hezbollah figura no topo da lista, com um capital de US$ 1,1 bilhão.

O Quadro 2 classifica a definição de lista os principais grupos terroristas na visão dos EUA.

Quadro 2 – Principais grupos terroristas listados pelo estado norte-americano

Data de inclusão	Grupo terrorista e respectiva sigla
10/8/1997	Abu Sayyaf Group (ASG)
10/8/1997	Aum Shinrikyo (AUM)
10/8/1997	Basque Fatherland and Liberty (ETA)
10/8/1997	Gama'a al-Islamiyya (Islamic Group - IG)
10/8/1997	HAMAS
10/8/1997	Harakat ul-Mujahidin (HUM)
10/8/1997	Hizballah
10/8/1997	Kahane Chai (Kach)
10/8/1997	Kurdistan Workers Party (PKK, aka Kongra-Gel)
10/8/1997	Liberation Tigers of Tamil Eelam (LTTE)
10/8/1997	National Liberation Army (ELN)
10/8/1997	Palestine Liberation Front (PLF)
10/8/1997	Palestine Islamic Jihad (PIJ)
10/8/1997	Popular Front for the Liberation of Palestine (PFLP)
10/8/1997	PFLP-General Command (PFLP-GC)
10/8/1997	Revolutionary Armed Forces of Colombia (FARC)
10/8/1997	Revolutionary People's Liberation Party/Front (DHKP/C)
10/8/1997	Shining Path (SL)
10/8/1999	al-Qa'ida (AQ)
9/25/2000	Islamic Movement of Uzbekistan (IMU)
5/16/2001	Real Irish Republican Army (RIRA)
12/26/2001	Jaish-e-Mohammed (JEM)
12/26/2001	Lashkar-e Tayyiba (LeT)
3/27/2002	Al-Aqsa Martyrs Brigade (AAMB)
3/27/2002	Asbat al-Ansar (AAA)
3/27/2002	al-Qaida in the Islamic Maghreb (AQIM)

(continua)

Quadro 2 (continuação) – Principais grupos terroristas listados pelo Estado norte-americano

Data de inclusão	Grupo terrorista e respectiva sigla
8/9/2002	Communist Party of the Philippines/New People's Army (CPP/NPA)
10/23/2002	Jemaah Islamiya (JI)
1/30/2003	Lashkar i Jhangvi (LJ)
3/22/2004	Ansar al-Islam (AAI)
7/13/2004	Continuity Irish Republican Army (CIRA)
12/17/2004	Islamic State of Iraq and the Levant (formerly al-Qa'ida in Iraq)
6/17/2005	Islamic Jihad Union (IJU)
3/5/2008	Harakat ul-Jihad-i-Islami/Bangladesh (HUJI-B)
3/18/2008	al-Shabaab
5/18/2009	Revolutionary Struggle (RS)
7/2/2009	Kata'ib Hizballah (KH)
1/19/2010	al-Qa'ida in the Arabian Peninsula (AQAP)
8/6/2010	Harakat ul-Jihad-i-Islami (HUJI)
9/1/2010	Tehrik-e Taliban Pakistan (TTP)
11/4/2010	Jundallah
5/23/2011	Army of Islam (AOI)
9/19/2011	Indian Mujahedeen (IM)
3/13/2012	Jemaah Anshorut Tauhid (JAT)
5/30/2012	Abdallah Azzam Brigades (AAB)
9/19/2012	Haqqani Network (HQN)
3/22/2013	Ansar al-Dine (AAD)
11/14/2013	Boko Haram
11/14/2013	Ansaru
12/19/2013	al-Mulathamun Battalion (AMB)
1/13/2014	Ansar al-Shari'a in Benghazi
1/13/2014	Ansar al-Shari'a in Darnah
1/13/2014	Ansar al-Shari'a in Tunisia
4/10/2014	ISIL Sinai Province (formerly Ansar Bayt al-Maqdis)
5/15/2014	al-Nusrah Front
8/20/2014	Mujahidin Shura Council in the Environs of Jerusalem (MSC)
9/30/2015	Jaysh Rijal al-Tariq al Naqshabandi (JRTN)
1/14/2016	ISIL-Khorasan (ISIL-K)
5/20/2016	Islamic State of Iraq and the Levant's Branch in Libya (ISIL-Libya)
7/1/2016	Al-Qa’ida in the Indian Subcontinent
8/17/2017	Hizbul Mujahideen (HM)
2/28/2018	ISIS-Bangladesh
2/28/2018	ISIS-Philippines
2/28/2018	ISIS-West Africa
5/23/2018	ISIS-Greater Sahara
7/11/2018	al-Ashtar Brigades (AAB)
9/6/2018	Jama'at Nusrat al-Islam wal-Muslimin (JNIM)

Fonte: Eua (2012).

O Quadro 3 apresenta a resolução de 4 de agosto de 2017 (UNIÃO EUROPEIA, 2017) que atualiza a lista de pessoas, grupos e entidades a que se aplicam os artigos da Posição Comum 2001/931/PESC relativa à aplicação de medidas específicas de combate ao terrorismo. Uma característica desta lista é a divulgação de nomes de pessoas e endereços para conhecimento público, aumentando a assim a percepção preventiva sobre o assunto.

Quadro 3 – Lista de terroristas da UE

Ordem	Nome e dados
1	ABDOLLAHI Hamed (também conhecido por Mustafa Abdullahi), nascido em 11 de agosto de 1960 no Irã. Número de passaporte: D9004878.
2	AL-NASSER, Abdelkarim Hussein Mohamed, nascido em Al Ihsa (Arábia Saudita); cidadão da Arábia Saudita
3	AL YACOUB, Ibrahim Salih Mohammed, nascido em 12.10.1966, em Tarut (Arábia Saudita); cidadão da Arábia Saudita
4	AL YACOUB, Ibrahim Salih Mohammed, nascido em 12.10.1966, em Tarut (Arábia Saudita); cidadão da Arábia Saudita
5	ARBABSIAR Manssor (também conhecido por Mansour Arbabsiar), nascido em 6 ou 15 de março de 1955 no Irã. Nacional iraniano e americano (EUA). Número de passaporte: C2002515 (Irã); Número de passaporte: 477845448 (EUA). Documento de identificação nacional n.o: 07442833, válido até 15 de março de 2016 (carta de condução EUA).
6	BOUYERI, Mohammed (também conhecido por Abu ZUBAIR, por SOBIAR e por Abu ZOUBAIR), nascido em 8.3.1978, em Amesterdão (Países Baixos).
7	EL HAJJ, Hassan Hassan, nascido em 22.03.1988, em Zaghdraiya, Sidon, Líbano, cidadão canadiano. Número de passaporte: JX446643 (Canadá). 3. IZZ-AL-DIN, Hasan (também conhecido por GARBAYA, Ahmed, por SA-ID e por SALWWAN, Samir), nascido em 1963, no Líbano; cidadão do Líbano.
8	MELIAD, Farah, nascido em 5.11.1980, em Sydney (Austrália), cidadão australiano. Número de passaporte: M2719127 (Austrália).
9	MOHAMMED, Khalid Shaikh (também conhecido por ALI, Salem, por BIN KHALID, Fahd Bin Adballah, por HENIN, Ashraf Refaat Nabith e por WADOOD, Khalid Adbul), nascido em 14.4.1965 ou em 1.3.1964, no Paquistão, passaporte n.o 488555.
10	MOHAMMED, Khalid Shaikh (também conhecido por ALI, Salem, por BIN KHALID, Fahd Bin Adballah, por HENIN, Ashraf Refaat Nabith e por WADOOD, Khalid Adbul), nascido em 14.4.1965 ou em 1.3.1964, no Paquistão, passaporte n.o 488555.
11	ŞANLI, Dalokay (também conhecido por Sinan), nascido em 13.10.1976, em Pülümür (Turquia).
12	ŞANLI, Dalokay (também conhecido por Sinan), nascido em 13.10.1976, em Pülümür (Turquia).
13	SHAHLAI Abdul Reza (também conhecido por Abdol Reza Shala'i, por Abd-al Reza Shalai, por Abdorreza Shahlai, por Abdolreza Shahla'i, por Abdul-Reza Shahlaee, por Hajj Yusef, por Haji Yusif, por Hajji Yasir, por Hajji Yusif e por Yusuf Abu-al-Karkh), nascido por volta de 1957 no Irã. Endereços: 1) Kermanshah, Irã; 2) Base Militar de Mehran, Província de Ilam, Irã.
14	SHAKURI, Ali Gholam, nascido por volta de 1965 em Teerã, Irã.
15	SOLEIMANI Qasem (também conhecido por Ghasem Soleymani, por Qasmi Sulayman, por Qasem Soleymani, por Qasem Solaimani, por Qasem Salimani, por Qasem Solemani, por Qasem Sulaimani e por Qasem Sulemani), nascido em 11 de março de 1957 no Irã. Cidadão do Irã. Número de passaporte: 008827 (diplomático do Irã), emitido em 1999. Título: Major-General.

Fonte: União_Europeia (2017).

No Quadro 4, estão disponíveis os grupos terroristas da EU.

Quadro 4 – Lista de grupos terroristas da UE

Ordem	Grupo terrorista
1	«Abu Nidal Organisation — ANO» (Organização Abu Nidal — «ANO») [(também conhecida por «Fatah revolutionary Council» («Conselho Revolucionário do Fatah»), por «Arab Revolutionary Brigades» («Brigadas Revolucionárias Árabes»), por «Black September» («Setembro Negro») e por «Revolutionary Organisation of Socialist Muslims» («Organização Revolucionária dos Muçulmanos Socialistas»)]
2	Al-Aqsa Martyr's Brigade» («Brigadas dos Mártires de Al-Aqsa»).
3	«Al-Aqsa e.V.».
4	«Babbar Khalsa».
5	«Communist Party of the Philippines» («Partido Comunista das Filipinas»), incluindo o «New People's Army» — «NPA» [Novo Exército Popular (NEP)], Filipinas.
6	«Gama'a al-Islamiyya» [(também conhecido por «Al-Gama'a al-Islamiyya», «Islamic Group» — «IG») («Grupo Islâmico» — «GI»)].
7	«Gama'a al-Islamiyya» [(também conhecido por «Al-Gama'a al-Islamiyya», «Islamic Group» — «IG») («Grupo Islâmico» — «GI»)].
8	«İslami Büyük Doğu Akıncılar Cephesi» — «IBDA-C» («Great Islamic Eastern Warriors Front») («Grande Frente Islâmica Oriental de Combatentes»).
9	«Hamas», incluindo o «Hamas-Izz al-Din al-Qassem».
10	«Hizballah Military Wing» («Ala Militar do Hezbolá») [também conhecida por «Hezbollah Military Wing», «Hizbullah Military Wing», «Hizbollah Military Wing», , «Hizb Allah Military Wing» e «Jihad Council», («Conselho da Jihad») (e todas as unidades sob a sua alçada, incluindo a «External Security Organisation») (Organização de Segurança Externa)].
11	«Hizbul Mujaïdine» — «HM».
12	«Khalistan Zindabad Force» — «KZF» («Força Khalistan Zindabad»).
13	«Kurdistan Workers' Party» — «PKK» («Partido dos Trabalhadores do Curdistão» — «PKK») (também conhecido por «KADEK» e por «KONGRA-GEL»).
14	«Liberation Tigers of Tamil Eelam» — «LTTE» («Tigres de Libertação do Elam Tamil» — «LTTE»).
15	«Ejército de Liberación Nacional» («Exército de Libertação Nacional»).
16	«Palestinian Islamiadc Jih» — «PIJ» («Jihad Islâmica Palestiniana» — «PIJ»).
17	«Popular Front for the Liberation of Palestine» — «PFLP» («Frente Popular de Libertação da Palestina» — «FPLP»).
18	«Popular Front for the Liberation of Palestine — General Command» («Frente Popular de Libertação da Palestina — Comando Geral») [(também conhecida por «PFLP — General Command») («FPLP — Comando Geral»)].
19	«Fuerzas armadas revolucionarias de Colombia» — «FARC» («Forças Armadas Revolucionárias da Colômbia — FARC»).
20	«Devrimci Halk Kurtuluş Partisi-Cephesi» — «DHKP/C» [(também conhecido por «Devrimci Sol» («Esquerda Revolucionária»), e por «Dev Sol»)] («Exército/Frente/Partido Revolucionário Popular de Libertação»).
21	«Sendero Luminoso» — «SL» («Caminho Luminoso»).
22	«Teyrbazen Azadiya Kurdistan» — «TAK» [também conhecido por «Kurdistan Freedom Falcons» e por «Kurdistan Freedom Hawks» («Falcões da Liberdade do Curdistão»)].

Fonte: União_Europeia (2017).

Conforme os quadros supracitadas, há prioridade nesse tipo de assunto e uma centralização de informações obtidas, por entender-se que isto é uma área

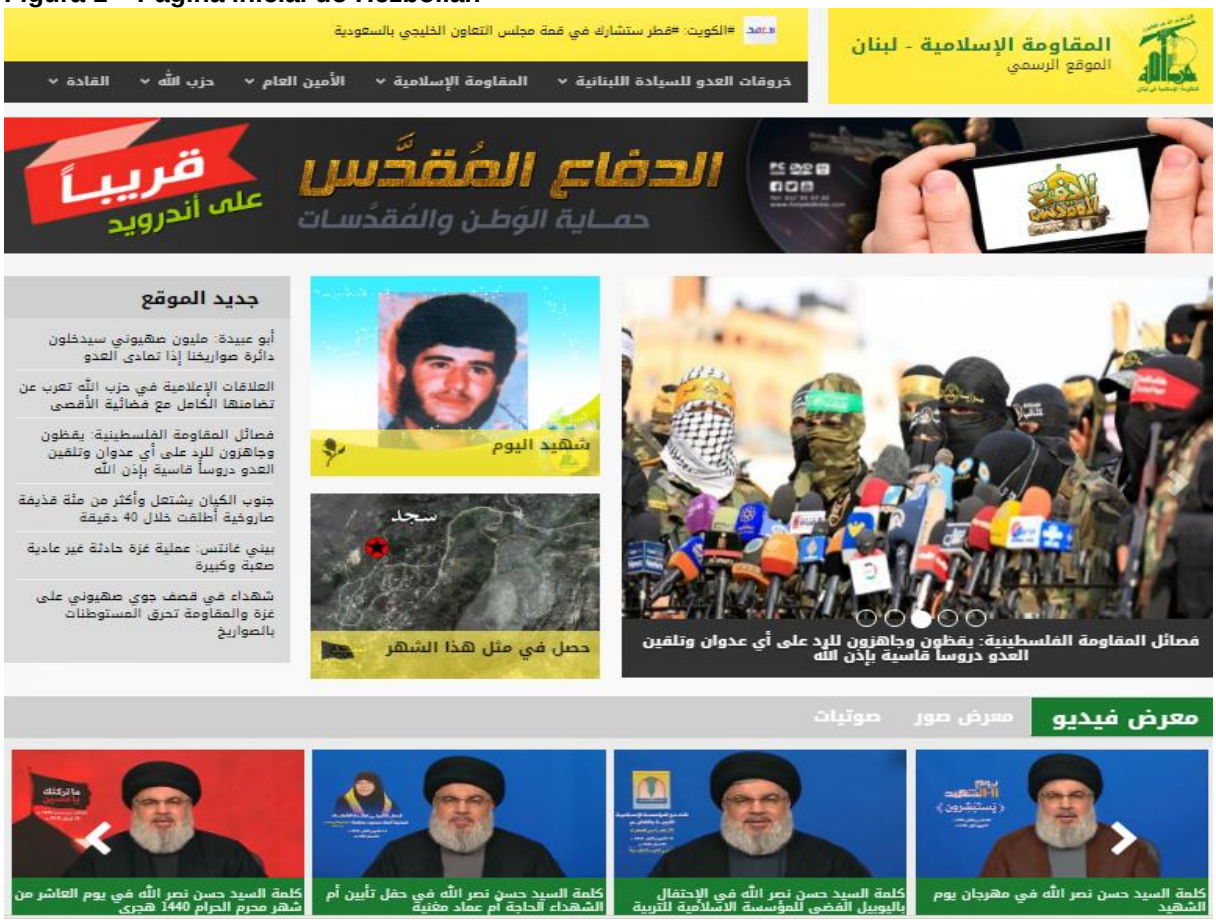
sensível e de salvaguarda nacional, com possibilidade de ações destes grupos. Essas ações podem ocorrer de uma forma mais caracterizada por atentados a bomba a multidões ou instalações, porém não é descartada a atuação destes mesmos grupos em um ataque no ambiente cibernético, o que caracteriza o terrorismo cibernético.

Dada essa relevância, a resposta que alguns países encontraram é justamente o monitoramento dos meios de comunicação, para uma pronta resposta, caso seja desencadeado um ataque desta natureza e pelas características deste ataque, identificar qual organização terrorista coordenou tal ação. Isso por que, uma das características do terrorismo, é que o terrorismo não possui face. Ele não mostra o rosto, motivo que historicamente seus ataques são desencadeados furtivamente. Não usam uniformes, salvo para propagar a propaganda ideológica por meio de sites ou outros meios de difusão, e seus integrantes convivem cotidianamente com a população.

Neste ponto o ambiente cibernético é ideal para coordenar ataques ou praticar atos ilícitos, pois a facilidade de recrutamento e, principalmente os recursos empregados são mínimos e menos dispendiosos. Por exemplo, com ferramentas como a *deep web*, é possível manter o anonimato e interligar agentes terroristas, promovendo uma barreira contra órgãos de segurança, para o rastreamento em tempo real de se evitar um ataque.

Os órgãos de segurança brasileiros não possuem uma atitude, como de outras nações, em divulgar grupos terroristas ou integrantes de forma ostensiva para a população, com a realização de medidas preventivas e de monitoramento dos meios de transmissão. Como exemplo, a Figura 1 – Página inicial do Hezbollah, e Figura 2 – Página inicial da Jihad Palestina, são retrato das páginas eletrônicas de grupos terroristas com a divulgação de seus atos.

Figura 1 – Página inicial do Hezbollah



Fonte: Hezbollah (2018).

Figura 2 – Página inicial da Jihad Palestina

Fonte: Jihad (2018).

2.3 SEGURANÇA DA INFORMAÇÃO (SI)

Neste estudo, a análise da segurança é um fator de relevância, pois é nela que qualquer tipo de ataque pode ser prevenido e, caso se obtenha êxito, a possibilidade de identificar os atores envolvidos. Por essa lógica, a informação de, uma maneira geral, representa um ativo, e demonstra os atributos necessários para a segurança da informação. “Considera **Ativo de informação.** Meios de armazenamento, transmissão e processamento, sistema de informação, bem como local onde se encontram esses meios e as pessoas que a eles têm acesso.” (BRASIL, 2017, p. 15).

A mesma fonte descreve os atributos clássicos de SI, que são os seguintes:

a) **confidencialidade**: propriedade de negar a disponibilização ou revelação da informação a indivíduos, entidades ou processos não autorizados nem credenciados;

b) **integridade**: propriedade de salvaguarda da exatidão e totalidade da informação, de forma a garantir que o conteúdo original da informação não seja modificado indevidamente por elemento humano ou qualquer outro processo;

c) **disponibilidade**: propriedade de assegurar que a informação esteja acessível e utilizável sob demanda de uma entidade autorizada;

d) **autenticidade**: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

e) **não-repúdio (irretratabilidade)**: propriedade de assegurar que, num processo de envio e recebimento de informações, nenhum participante originador nem destinatário de informação possa, em um momento posterior, negar a respectiva atuação

Em apresentação realizada por Hoepers (2014), são ancorados dois pilares básicos para a SI:

1) Privacidade: habilidade e/ou direito de proteger suas informações pessoais, estende-se à habilidade e/ou direito de prevenir invasões do seu espaço pessoal;

2) Confidencialidade: envolve a obrigação de proteger os segredos de outras pessoas ou organizações, se você souber deles (www.cert.br).

Para conseguir uma segurança razoável tem-se tentado atingir os seguintes objetivos:

- detectar comprometimentos o mais rápido possível;
- diminuir o impacto;
- conter, mitigar e recuperar de ataques o mais rápido possível.

Um meio preventivo é que, mesmo sob um ataque, os meios devem funcionar, criando uma resiliência. Conforme Hoepers (2014), resiliência significa:

> - identificar o que é crítico e precisa ser mais protegido;
> - definir políticas (de uso aceitável, acesso, segurança etc.);
> - treinar profissionais para implementar as estratégias e políticas de segurança;
> - treinar e conscientizar os usuários sobre os riscos e medidas de segurança necessários;
> - implantar medidas de segurança que implementem as políticas e estratégias de segurança e aplicar correções ou instalar ferramentas de segurança;
> - formular estratégias para gestão de incidentes de segurança e formalizar grupos de tratamento de incidentes.

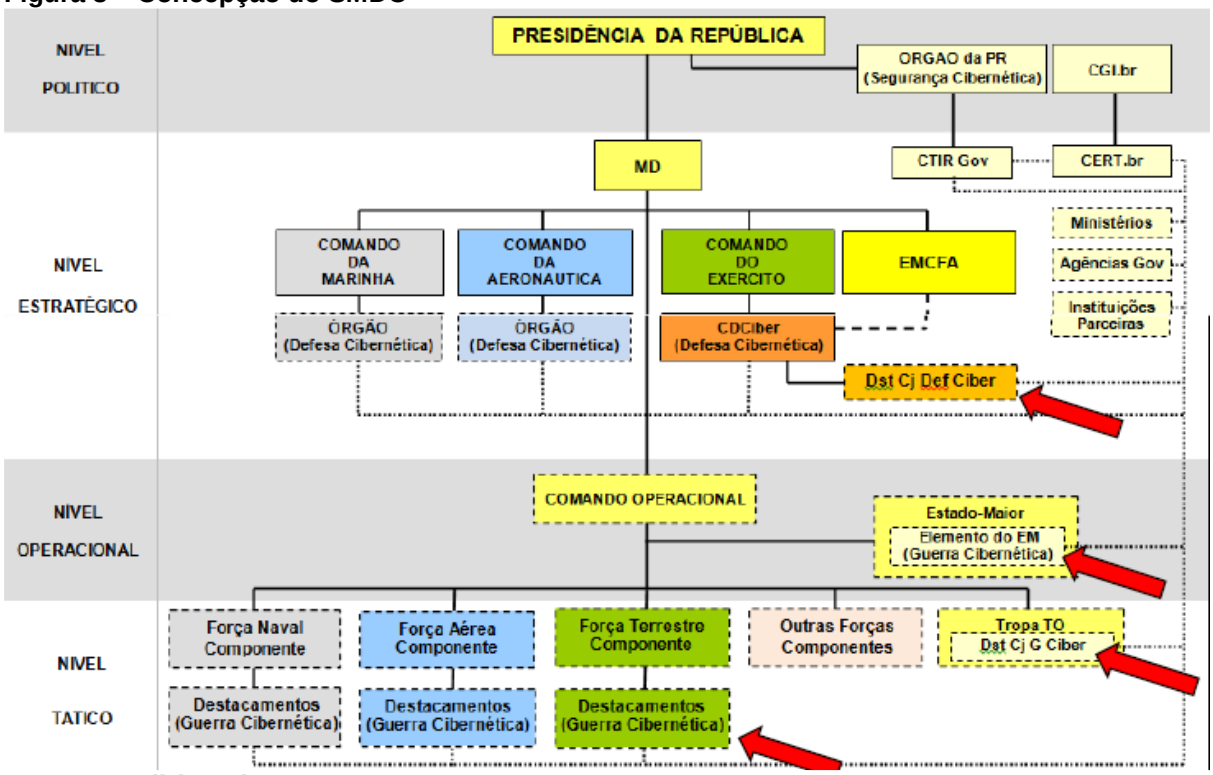
2.4 SISTEMA MILITAR DE COMANDO E CONTROLE DE DEFESA CIBERNÉTICA

O Ministério da Defesa (MD) considera que a SI está estruturada em um Sistema Militar de Comando e Controle (SISMC²). De acordo com o Manual MD31-P-03 (BRASIL, 2017, p. 17), SI:

> É o conjunto de ações que objetivam viabilizar e assegurar a proteção das informações e dos ativos de informação, de modo a permitir a utilização eficaz e eficiente de seus serviços somente a usuários autorizados, bem como impedir a intrusão e a modificação desautorizada de dados ou informações armazenados, em processamento ou em trânsito.

Dentro desta estrutura, coube ao Centro de Defesa Cibernética (CDCiber) estruturar o Sistema Militar de Defesa Cibernética (SMDC) (Figura 3).

Figura 3 – Concepção do SMDC



Fonte: Brasil (2014).

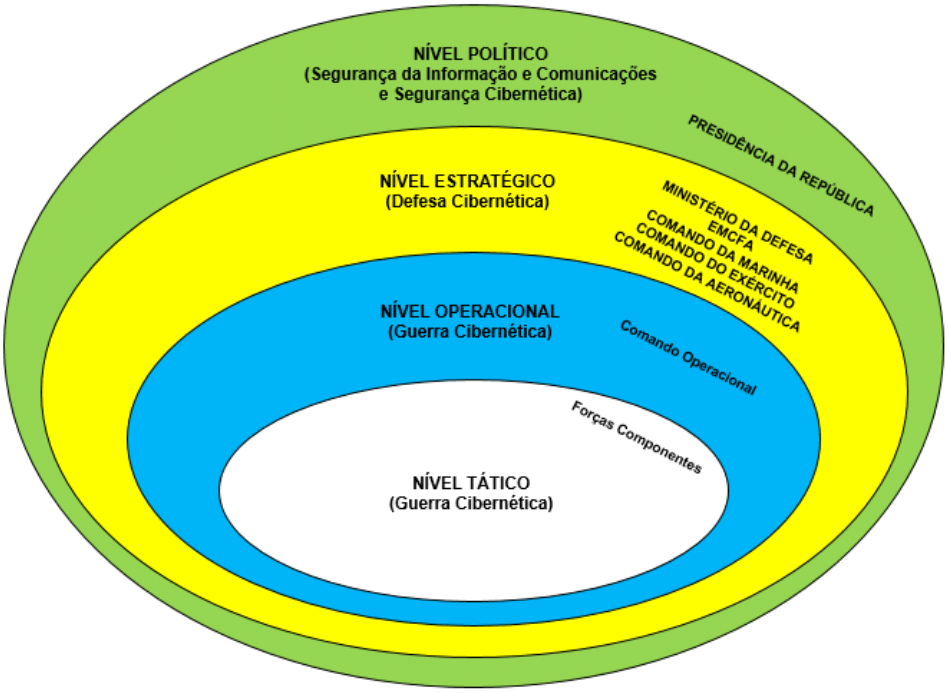
Conforme a figura demonstra, o SMDC faz parte do C², é dividido em níveis, e esses níveis estão em uma estrutura hierarquizada, tendo como agentes participantes toda a estrutura *web* do território nacional. Nesse contexto, o Manual de Defesa Cibernética (BRASIL, 2017) norteia as seguintes denominações, de acordo com o nível de decisão, conforme apresentado na Figura 4:

a) nível político – Segurança da Informação e Comunicações (SIC) e Segurança Cibernética – coordenadas pela Presidência da República e abrangendo a Administração Pública Federal (APF) direta e indireta, bem como as infraestruturas críticas da informação inerentes às infraestruturas críticas nacionais;

b) nível estratégico – Defesa Cibernética – a cargo do MD, Estado-Maior Conjunto das Forças Armadas (EMCFA) e comandos das Forças Armadas (FA), interagindo com a Presidência da República e a APF; e

c) níveis operacional e tático – Guerra Cibernética – denominação restrita ao âmbito interno das FA.

Figura 4 – Níveis de estratégias



Fonte: Brasil (2017, p. 17).

2.5 DEPARTAMENTO DE SEGURAÇÃO DA INOFRMAÇÃO E COMUNICAÇÕES (DSIC)

Aliado à estrutura do Ministério da Defesa, o DSIC, órgão vinculado ao Gabinete de Segurança Institucional da Presidência da República, possui as atividades apresentadas no Quadro 5.

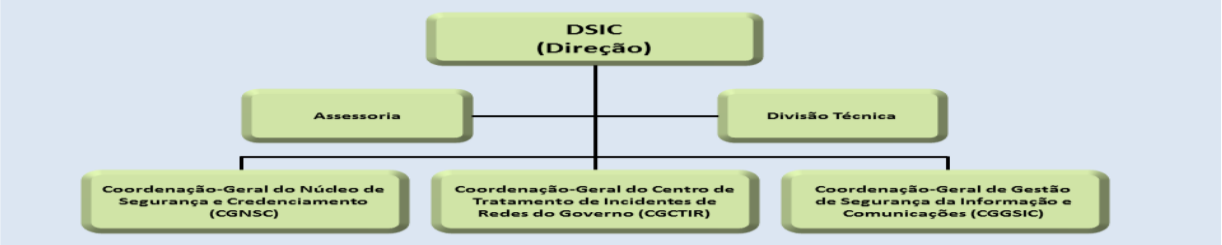
Quadro 5 – Missão do DSIC

	Atividade
1	Exercer, por meio do Núcleo de Segurança e Credenciamento, atividades relacionadas ao credenciamento de segurança e ao tratamento de informação sigilosa;
2	Planejar, orientar, coordenar e desenvolver as políticas e ações de segurança da informação no âmbito da APF;
3	Definir requisitos metodológicos para a implementação de ações de segurança da informação e comunicações, incluídas as de segurança cibernética e de segurança das infraestruturas críticas da informação do Estado, pelos órgãos e entidades da APF;
4	Operacionalizar e manter centro de tratamento de incidentes ocorridos nas redes de governo;
5	Estudar legislações correlatas e implementar as propostas sobre matérias relacionadas à segurança da informação;
6	Avaliar tratados, acordos ou atos internacionais relacionados à segurança da informação e ao tratamento e à troca de informação sigilosa;
7	Acompanhar o desenvolvimento da Política Nacional de Segurança da Informação e promover ações para sua implementação;
8	Realizar outras atividades determinadas pelo Ministro de Estado, pelo Secretário-Executivo e pelo Secretário da SCS.

Fonte: Adaptado de Brasil (20--).

Já o organograma do DSIC é organizado da forma como apresentada na Figura 5.

Figura 5 – Organograma do DSIC



Fonte: Brasil (20--).

3 CIBERNÉTICA E SUAS ANÁLISES

Uma das definições acerca da cibernética, conforme Salomão (2007), é:

> (…) dada por Norbert Wiener quando promoveu a publicação de seu livro, Cibernética, em 1945, pode ser descrita pela seguinte sentença: “A ciência do controle e da comunicação no animal e na máquina”.
> (…)
> Outro fato a ser destacado da definição de Wiener é a classificação da Cibernética como ciência. Agregar a um novo campo de estudos o título de ciência traz consigo uma enorme carga de significados e conceitos, que a suposta nova ciência deve contemplar. Todavia, no momento em que a cibernética emerge, para estabelecê-la como uma ciência era preciso respeitar o principio básico do discurso científico: a separação entre o observador e o que é observado, já que a objetividade se define pela não-interferência das características do observador na descrição dos itens observados (FOERSTER, 1994). Além disso, uma ciência precisa ter definido seu objeto de estudo e deve trabalhar com conceitos sólidos e indubitáveis. Pois bem, a Cibernética possui como principal objeto de estudo os sistemas (PASK, 1961), e possui claramente conceitos bem definidos, que estabelecem uma clara ligação e dependência entre si (SALOMÃO, 2007, p. 2).

Sob a ótica de a Grenz e Smith (2005, s/p), cibernética é “A ciência do controle e da comunicação do modo como se relaciona com os mecanismos, indivíduos e sociedades. Ela deriva do termo grego *kybernetes*, que significa ‘timoneiro’”. Nesse sentido, inclui os vários tipos de processos que dependem da troca e do fluxo de informações. Um recurso cibernético é um mecanismo ou sistema que processa informações, tais como um computador ou o sistema de telecomunicações. O estudo da cibernética levanta um sem-número de questões éticas das quais a primeira é o desenvolvimento da Inteligência Artificial (IA) e suas implicações para o que ela considera um ser vivo (GRENZ; SMITH, 2005).

A definição se integra a muitos autores e acadêmicos, em que a cibernética é uma ciência que rege o controle e a forma de comunicação entre seres vivos e máquinas, em diferentes meios e processos.

3.1 CIBERNÉTICA E TERRORISMO

No meio cibernético, a difusão de vírus ou invasões para roubo de dados, sequestro de informações entre outros atos ilícitos, ligados a grupos criminosos ou atores isolados, recebem no fim ou no transcorrer de seus atos, uma atenção específica da mídia. A rapidez com que esses atos ocorrem faz com que nem

mesmos os órgãos de segurança ou de controle sejam capazes de prevenir e tomar medidas preventivas para minimizar ou evitar sua propagação. Nessa lógica, o terrorismo cibernético possui o mesmo vetor de uma ação terrorista física, a difusão de sua propaganda ideológica.

Na análise de Gardini (2014), o uso do poder do espaço cibernético por organizações terroristas já vêm ocorrendo há algum tempo. Um dos primeiros casos documentados de um ataque contra um sistema de computadores de um Estado por um grupo terrorista foi no Sri Lanka, em 1998, pelo grupo *Tamil Tigers*, no qual embaixadas do país pelo mundo foram bombardeadas por semanas com 800 *e-mails* ao dia, trazendo a mensagem "Nós somos os Tigres Negros da internet, e nós vamos romper seus sistemas de comunicação." (SIBONI; COHEN; ROTBART, 2013, p. 20).

De acordo com o documento "The use of internet for terrorists purposes", do Escritório das Nações Unidas sobre Drogas e Crimes (UNODC, 2012), existem seis meios pelos quais terroristas podem utilizar o ciberespaço: propaganda, financiamento, treinamento, planejamento, execução e ataques cibernéticos. A propaganda é a forma que esses grupos disseminam seus ideais, recrutam novos membros e incitam ações terroristas, sendo o espaço cibernético o meio ideal para isso. A velocidade de informação e facilidade de se manter no anonimato ajudam a propagar, "(…) isso pode incluir mensagens virtuais, apresentações, revistas, tratados, arquivos de áudio e vídeo e jogos desenvolvidos por organizações terroristas ou simpatizantes." (UNODC, 2012, p. 3, *tradução livre*) Atualmente, a propaganda é utilizada por muitos grupos terroristas, principalmente para ensinar sua doutrina e conquistar novos membros. Um exemplo é o aplicativo *The Dawn of Glad Tidings*, que oferece aos usuários informações sobre o grupo "Estado Islâmico." (TROWBRIDGE, 2014).

Nessa perspectiva, termos como 'Guerra cibernética, Ciberterrorismo, Guerra de Dados, Guerra de Informação, Ciberguerra, terrorismo cibernético', convergem para o mesmo ponto: o uso de dados e seus meios de transmissão para causar danos a equipamentos ou pessoas. Além disso, busca-se que esse tipo de ataque tenha seu objetivo consolidado em larga escala.

Sendo assim, Baptista (2016), define ciberterrorismo como:

> (…) um ataque deliberado e motivado por questões ideológicas, políticas ou religiosos contra sistemas de informação ou infraestruturas de TI com a

> finalidade de interromper serviços essenciais como o fornecimento de água, energia, serviços de emergência e hospitalares, sistemas financeiros, controle de tráfego aéreo e semelhantes. Ataques ciberterroristas, para serem considerados como tal, devem incutir o terror, como comumente entendido, isto é, ter como resultado mortes e/ou destruição em larga escala, e devem ter uma motivação política, ideológica ou religiosa. A simples utilização de computadores pelos terroristas como um facilitador de suas atividades, seja para propaganda, recrutamento, mineração de dados, comunicação ou outros fins, não é ciberterrorismo.

Já Pinto (2011, p. 7) descreve ciberterrorismo como:

> Actos fundados em motivações políticas, ideológicas ou sociais e em operações de *hacking* com o objectivo de causar prejuízos severos (perda de vidas humanas, prejuízos econômicos, ataques ou ameaças contra sistemas informáticos, redes e a respectiva Informação neles armazenada) de forma a intimidar ou coagir um governo. Pode chegar a ser um ataque físico com o objectivo de destruir nos computorizados de infraestruturas criticas (internet, telecomunicações) ou a grelha elétrica de um país ou de uma cidade. O Ciberterrorismo é semelhante ao cibercrime, mas é uma versão mais extrema do cibercrime, com consequências piores. Não existe uma definição normalizada (*standard*) de Ciberterrorismo e de ciberterrorista, que agrade a todos, pois a diferença entre *hacking* normal e Ciberterrorismo depende apenas da motivação do ataque (politico ou pessoal). Ou seja, quando é pessoal ocorre apenas um ataque de *hacking*, mas se houver outras motivações poderá passar a ser considerado um acto ciberterrorista. Independentemente da motivação, ambos podem ser punidos pelo *Computer Fraud and Abuse Act*[1] dos EUA. Na Europa existe uma tentativa de harmonização entre as leis da União Europeia e dos EUA, o que significa que existem muitas semelhanças nas leis aprovadas e em vigor.

Ainda na mesma linha, a expressão Terrorismo Cibernético, segundo Barreto (2017, p. 63) que:

> refere-se ao emprego, por terroristas, de técnicas de destruição ou incapacitação de redes computacionais de informação. Entre essas redes, destaca-se a internet, em razão do seu crescente fluxo de informações, importância, abrangência e extensão geográfica.
> Por isso, especialistas em Terrorismo Cibernético costumam apoiar-se na concepção de cenários possíveis, mediante avaliações feitas a partir da quantificação das (1) vulnerabilidades conhecidas e existentes nos sistemas informatizados, das (2) ameaças hipotéticas e reais que sobre eles incidem, e, finalmente, do (3) valor estratégico, político ou econômico das informações operadas nesses sistemas.

[1] "O *Computer Fraud and Abuse Act* é uma lei Americana aprovada pelo Congresso dos Estados Unidos em 1986 com o objectivo de diminuir o *hacking* e *cracking* de sistemas informáticos e para lidar com crimes relacionados com sistemas informáticos do governo. Esta lei sofreu varias alterações ao longo dos anos para se adequar a realidade do momento." (PINTO, 2014, p. 38).

Para que este tipo de atividade seja estruturada e consolidada, é necessário pessoas capacitadas e com conhecimento na área. Nesse sentido, Nunes (2004, p. 7) afirma que:

> (…) o facto de o custo de entrada associado ao desenvolvimento de acções mais disruptivas que as básicas e tradicionais actividades de *hacking* ser geralmente muito alto e que falta, à generalidade das organizações e grupos terroristas, o capital humano e a capacidade para montar uma operação de ciberterrorismo com alguma relevância. O tempo estimado para um grupo terrorista levantar uma capacidade de ciberterrorismo de raiz, até atingir o nível avançado/estruturado, é de 2-4 anos e para atingir o nível complexo/coordenado de 6-10 anos. No entanto, esse tempo poderá ser significativamente reduzido se for seguido um processo de *outsourcing*, como alguns dados recentemente recolhidos parecem indicar (DENNING, 2000). O ciberterrorismo poderá assim ser considerado uma ameaça, de impacto futuro mais consistente do que o que actualmente apresenta, posicionando-se como uma ferramenta auxiliar de importância crescente para o terrorismo transnacional.

Como visto há uma necessidade de suporte para que a ação tenha um grau de probabilidade de acontecimento. Nesse sentido, uma observação pertinente foi descrita por Pinto (2011).

> E necessário diferenciar entre o suporte e aos ataques. O suporte/actividade e o uso ilícito de SI por terroristas, sem o objectivo claro de causar efeitos coercivos numa audiência alvo, servindo mais para ampliar o impacto de outros actos terroristas. O Ciberterrorismo pode então ser classificado em actos/ataques ou actividades/suporte visto que para realizar um acto de Ciberterrorismo são necessárias varias actividades que incluem e não estão limitadas a recolha de Informações, comunicações, logística e abastecimento. O resultado final do uso de tecnologias de Informação e o que determina se os incidentes são ataques ou suporte, sendo os ataques uma forma de intimidar ou coagir directamente de acordo com as metas do grupo atacante. Por sua vez, o suporte destina-se a aumentar algum outro acto ou ameaça podendo ser terrorismo tradicional ou Ciberterrorismo.

3.2 CONCEITOS BÁSICOS DE CONFLITOS CIBERNÉTICOS

Em virtude da evolução da transmissão de dados e suas aplicações nos meios de controle de grandes estruturas nacionais, como usinas hidroelétricas, centrais de distribuição de energia, empresas de saneamento e distribuição de água, as quais são denominadas ‘pontos sensíveis’; a administração pública entende que ataques cibernéticos ou falhas de transmissão de dados que interligam esses pontos podem provocar efeitos bem desastrosos para um país. Esse tema passou a ter uma

atenção especial do MD e da Casa Civil, os quais iniciaram estudos para criar uma doutrina de defesa em caso de uma instabilidade gerada por ataque cibernético.

Nesse quesito, o *Manual de Guerra Cibernética* (BRASIL, 2017, p. 2) do Exército Brasileiro (EB), classifica os seguintes tópicos em um cenário de conflito cibernético (Quadro 6).

Quadro 6 – Possíveis cenários de conflito cibernético

CONFLITO	EXPLICAÇÃO
Ameaça cibernética	Causa potencial de um incidente indesejado, que pode resultar em dano ao espaço cibernético de interesse.
Artefato cibernético	Equipamento ou sistema empregado no espaço cibernético para execução de ações de proteção, exploração e ataque cibernéticos.
Ativos de informação	Meios de armazenamento, transmissão e processamento de dados e informação, os equipamentos necessários a isso (computadores, equipamentos de comunicações e de interconexão), os sistemas utilizados para tal, os sistemas de informação de um modo geral, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.
Cibernética	Termo que se refere à comunicação e controle, atualmente relacionado ao uso de computadores, sistemas computacionais, redes de computadores e de comunicações e sua interação.
Defesa cibernética	Conjunto de ações ofensivas, defensivas e exploratórias, realizadas no espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo MD, com as finalidades de proteger os sistemas de informação (Sist Info) de interesse da defesa nacional, obter dados para a produção de conhecimento de inteligência e comprometer os sistemas de informação do oponente.
Espaço cibernético	Espaço virtual composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam e são processadas e/ou armazenadas.
Fonte cibernética	Recurso que possibilita a obtenção de dados no espaço cibernético, utilizando-se ações de busca ou coleta, normalmente realizadas com auxílio de ferramentas computacionais. A fonte cibernética poderá ser integrada a outras fontes (humanas, imagens e sinais) para produção de conhecimento de inteligência.
Guerra cibernética	Corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar capacidades de C2 AO adversário, explorá-las, corrompê-las, degradá-las ou destruí-las, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de TIC para desestabilizar ou tirar proveito dos sistemas de informação do oponente e defender os próprios Sist Info. Abrange, essencialmente, as ações cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação às TIC.
Infraestrutura crítica da informação	Subconjunto dos ativos de informação que afeta diretamente a consecução e a continuidade da missão do estado e a segurança da sociedade.
Poder cibernético	Capacidade de utilizar o espaço cibernético para criar vantagens e eventos de influência neste e nos outros domínios operacionais e em instrumentos de poder.
Resiliência cibernética	Capacidade de manter as infraestruturas críticas da informação operando sob condições de ataque cibernético ou de restabelecê-las após uma ação adversa.

Fonte: Adaptado de Brasil (2017).

3.3 MEIOS UTILIZADOS EM ATAQUES CIBERTERRORISTAS E O NÍVEL DE SEUS OPERADORES

As formas de emprego para o ciberterrorismo seguem um padrão utilizado por *hackers*, *crackers* e outros agentes. São considerados de maior relevância os seguintes (PINTO, 2011): vírus, *worms*, trojans, *spyware,* Spam, *pishing* e botnets.

Há ainda outros processos para acesso ao objetivo do terrorista, sejam eles para despertar no subconsciente de possíveis seguidores a concordância de seus ideais e outros como: domínios expirados, jogos de computador, músicas, *firmware* e Engenharia Social.

Analisando o perfil dos agentes perpetuadores, eles se classificam nos seguintes apresentados no Quadro 7.

Quadro 7 – Perfil dos agentes

Agente	Nível	Objetivo
Amador	Baixo	Fins lucrativos em terceiros
Hacker	Intermediário	Encara como desafio suas ações
Cracker	Alto	Possui alto conhecimento técnico
Ativista	Baixo	Mobilização de opinião pública (vetor)
Crime organizado	Intermediário	Usa o meio cibernético para prática de ilícitos
Terrorista	Intermediário	Propagação de seus atos
Estado	Alto	Controle nos meios de transmissão

Fonte: Pinto (2011).

3.4 PERFIL E TIPOS DE MOTIVAÇÕES TERRORISTAS

O princípio do terrorismo sempre inicia com uma causa, normalmente do lado que se considera mais oprimida, diante daquele que possui a dominância de um estado. Ele agrega a sua causa uma ideologia em vetor que justificará as ações que se consolidarão à medida que a ‘causa’ ganha forma, adeptos e a propaganda de suas ações se difunde. Nesse sentido, um exemplo refere-se aos grupos terroristas islâmicos que possuem como base para os seus atos o livro do Alcorão, as ações terroristas do atentado do dia 11 de setembro nos Estados Unidos da América (EUA), tiveram fundo jihadista, perpetrado pelo grupo Al-qaeda, tendo seu mentor Osama Bin Laden filosofia, mentores.

Quando se trata do assunto perfil de um terrorista, imediatamente vem a figura de um elemento com traços físicos que remota aos árabes, com um turbante e um cinto de explosivos na cintura. A tese de Pinto (2011) avalia que:

> Os Ciberterroristas são normalmente jovens do sexo masculino, alguns com habilitações acadêmicas elevadas (Mestrados ou Doutoramentos), que tem a consciência de estar a violar a lei desrespeitando as normas sociais, a ordem e os sistemas de controlo social. Eles diferem dos criminosos comuns em pelo menos quatro características fundamentais:
> (1) Efectuam crimes de forma mais violenta;
> (2) Tem como meta infligir medo numa população alvo enorme;
> (3) Servem uma agenda social enorme tentando recrutar mais elementos para a causa deles;
> (4) Tentam conseguir uma exposição máxima aos media.
> A natureza do Ciberterrorismo pode ter em vista:
> (1) Desestabilizar Estados soberanos para alcançar uma maior forca de influencia numa certa região;
> (2) Causar uma visibilidade internacional para problemas persistentes como e o caso da Palestina, de forma a conseguir maior afecto;
> (3) Retaliar contra Estados soberanos em certas regiões que são encarados como sendo inimigos;
> (4) Minar a influencia de forcas mais poderosas que estejam a operar na região.
> O terrorismo crê em uma causa, e a causa, tem origem diversa no mundo utópico.

Discorrendo ainda sobre essa tese:

> (…) dada uma quase infinita variedade de circunstâncias em torno dos eventos terroristas, cada acto relacionado com as definições convencionais de terrorismo é único em vários aspectos, embora existam dimensões que distingam alguns terroristas, grupos terroristas e actos terroristas da maioria dos outros. Então, certos grupos de terroristas e actos individuais encaixam-se nas seguintes dimensões em que a variação de comportamentos nas várias dimensões pode ser maior que numa em particular.

E cita as seguintes motivações (PINTO, 2011, p. 43):

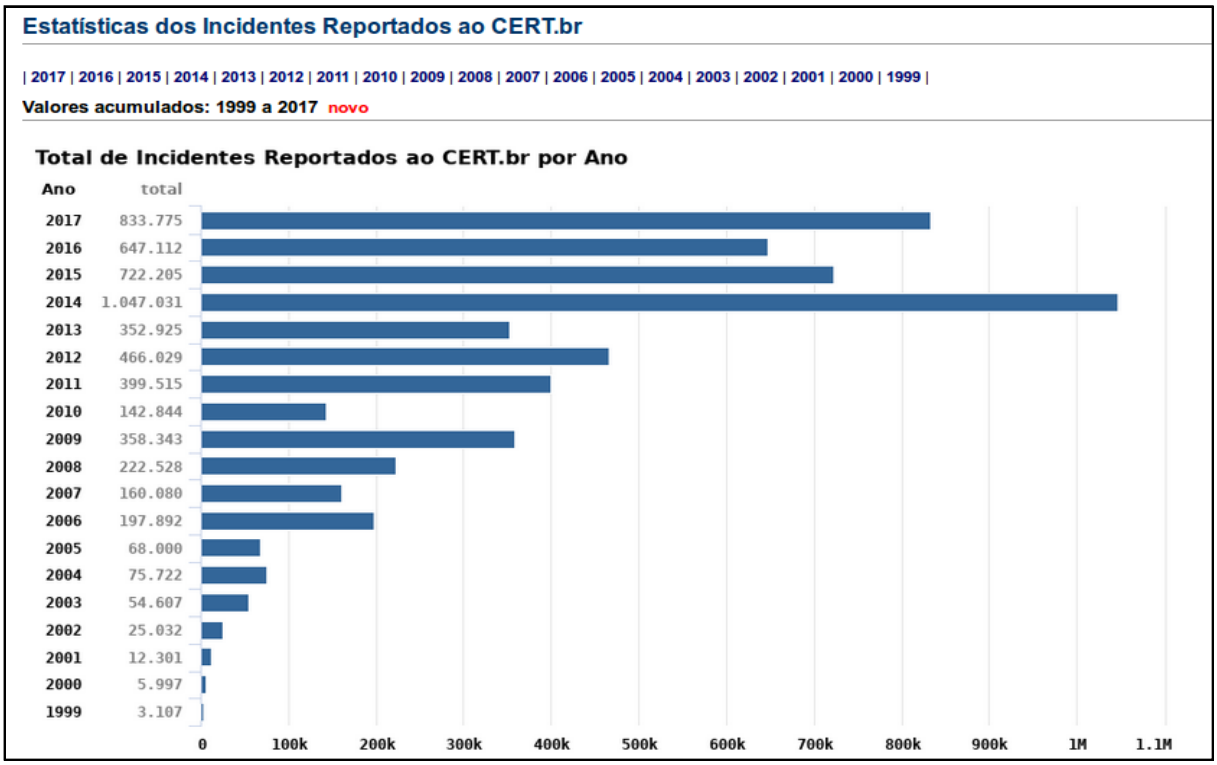
- politicamente motivadas;
- opera sob a autoridade de um Estado;
- grau de associação com redes ou outras organizações terroristas superiores;
- extensão da organização e planeamento;
- justificativas religiosas ou étnicas;
- os destinos dos alvos são civis ou simbólicos.

3.5 GRÁFICOS DE ATAQUES REGISTRADOS NO BRASIL

O CERT.br publica em seu sítio eletrônico dados estatísticos de ataques registrados no território brasileiro: Figura 6 – Estatísticas dos incidentes reportados, e Figura 7 – Estatísticas de notificações de spam reportadas; que vem subindo anualmente, conforme Diniz (2018):

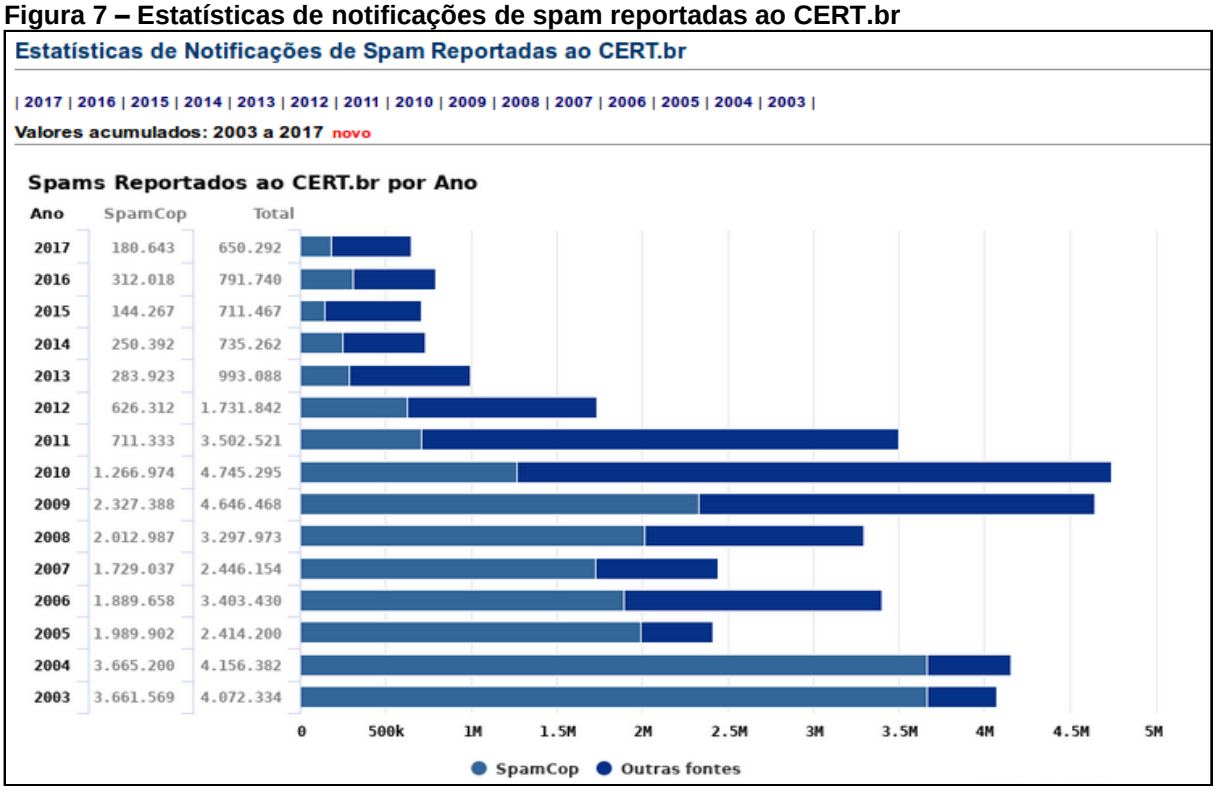
> Ataques digitais cresceram 29% no Brasil em 2017
>
> O número de incidentes relacionados a DDoS originados pelo avanço da internet das coisas foi quatro vezes maior que o de 2016.
> O número de ataques digitais **cresceu 29%** no ano passado em relação à 2016, totalizando 833.755 casos relatados ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) do Núcleo de Informação e Coordenação do Ponto BR (NIC.br). Os dados foram divulgados nesta terça-feira (20) pelo órgão.
>
> O número de incidentes de segurança reportados é o **segundo maior** desde 1999, quando os ataques digitais começaram a ser registrados. O ano com maior número de casos foi 2014 com 1.043.031 registros. Um dos motivos para o aumento expressivo de incidentes estaria no **avanço da internet das coisas (IoT)**.
>
> Do total de casos de 2017, 220.188 foram relacionados a dispositivos IoT que receberam **ataques de negação de serviço (DDoS)**. Esse número é **quatro vezes maior** do que o registrado em 2016, quando houve 60.432 ataques desse tipo. Diferentemente de ataques comuns de hackers, que invadem o sistema e podem prejudicar um determinado site com essa invasão, o DDoS resulta na invalidação desse site por sobrecarga. Ou seja, um alto tráfego forçado e manipulado que faz com que a página saia do ar.
>
> O maior ataque DDoS da história aconteceu na primeira semana desse mês e foi com uma operadora de telecomunicações dos Estados Unidos.Parte dos ataques DDoS também foi originada por **roteadores e modems de banda larga**, seja porque estavam comprometidos ou porque possuíam serviços mal configurados, permitindo amplificação de tráfego. O Centro de Estudo também apontou que ataques de força bruta a serviços como SSH (22/TCP) e TELNET (23/TCP) continuam muito frequentes e englobam tentativas de comprometer **dispositivos IoT e equipamentos de rede alocados às residências**, tais como modems ADSL e cabo, roteadores Wi-Fi, entre outros. Esse tipo de ataque visa adivinhar, por tentativa e erro, as suas senhas de administração e, assim, comprometer os dispositivos. (DINIZ, 2018, *grifos da autora*).

Figura 6 – Estatísticas dos incidentes reportados ao CERT.br



Fonte: Cert.br (2018).

Figura 7 – Estatísticas de notificações de spam reportadas ao CERT.br



Fonte: Cert.br (2018).

4 LEGISLAÇÃO E ÓRGÃOS COORDENADORES DE DEFESA CIBERNÉTICA

4.1 ESTRATÉGIA NACIONAL DE DEFESA – LIVRO BRANCO

Criado em 2008 e aprovado em 2012, a função do Livro Branco é integrar a Casa Civil, por meio da Presidência da República, com o MD em tratativas sobre as questões de cibersegurança no Brasil.

> O Livro Branco de Defesa Nacional (LBDN) é o mais completo e acabado documento acerca das atividades de defesa do Brasil. Abrangente, visa esclarecer a sociedade brasileira e a comunidade internacional sobre as políticas e ações que norteiam os procedimentos de segurança e proteção à nossa soberania. Além de aportar transparência quanto à atuação das Forças Armadas, prestando contas sobre a adequação da estrutura de defesa disponível no país, serve de instrumento para estimular o debate sobre esse tema no âmbito do Congresso Nacional, da burocracia federal, da Academia e da sociedade em geral (BRASIL, 2012).

O item 3.6 da END (BRASIL, 2012) prescreve que “Para que o desenvolvimento e a autonomia nacionais sejam alcançados é essencial o domínio crescentemente autônomo de tecnologias sensíveis, principalmente nos estratégicos setores espacial, cibernético e nuclear”. Ainda acerca do tema, o tópico 3.17 afirma que:

> Para se opor a possíveis ataques cibernéticos, é essencial aperfeiçoar os dispositivos de segurança e adotar procedimentos que minimizem a vulnerabilidade dos sistemas que possuam suporte de tecnologia da informação e comunicação ou permitam seu pronto restabelecimento. (BRASIL, 2012, p. 34)

A partir do estabelecimento do setor cibernético, decorrente da aprovação da END, em 2008, dois campos distintos passaram a ser reconhecidos: a segurança cibernética, a cargo da Presidência da República, e a defesa cibernética, a cargo do MD, por meio das FA.

4.2 CIBERDEFESA E INTEGRIDADE NACIONAL

Nos últimos vinte anos foi notória a participação brasileira em grandes eventos mundiais, por exemplo, a Copa FIFA 2014 e os Jogos Olímpicos 2016, os quais reforçaram o país como potência no continente sul-americano. Isso fez com

que o Brasil se tornasse um alvo em potencial de ataques cibernéticos oriundos de diversas partes do globo. Essas atividades trouxeram à luz o controle sobre possíveis ataques em áreas com grande quantidade de público ou danos em estruturas físicas.

Nesse sentido, a promulgação da END, anterior a esses grandes eventos, obrigou as FA e os demais órgãos de segurança a olharem com mais atenção ao que estava ocorrendo em outras nações e o que poderia ocorrer aqui, bem como quais seriam seus reflexos tanto em questões de soberania nacional e principalmente na projeção do país pelo mundo. (MACHADO et al., 2017).

Com a realização da Copa FIFA 2014, houve uma unificação de todas as cidades sede, através de uma rede integrada de segurança, com uma rede exclusiva de tráfego de dados, as quais se denominaram CDA – Centro de Controle de Área a experiência bem sucedida nos eventos Copa FIFA 2014, em virtude do controle de todos os escalões de segurança terem sido unificados e coordenados em áreas nas quais ocorreriam os jogos por comandantes das FA, observação está feita no trabalho de Silva (2017, p. 18):

> Dentro desse contexto situacional, a partir de experiências anteriores, como os jogos Pan-Americanos, no ano de 2007, os Jogos Mundiais Militares, no ano de 2011, a Conferência Mundial Rio +20, no ano de 2012 e a Jornada Mundial da Juventude, no ano de 2013, ficou evidente a necessidade de uma equipe de coordenação de segurança que pudesse contribuir de forma consubstancial no entendimento do que viesse a ser os Grandes Eventos, bem como as suas peculiaridades. No entanto, esse novo desafio criou um cenário extremamente complexo, pois haveria espectadores, delegações, comitivas e chefes de Estado de vários países. Logo, promover a integração, a organização e a interoperabilidade de recursos humanos e materiais, visando à obtenção de um ambiente pacífico e seguro para a realização desse evento, tornou-se outro grande obstáculo a ser transposto. Dessa forma, por decisão presidencial, o Ministério da Defesa foi inserido como um dos componentes das forças de segurança pública para Grandes Eventos, apoiando os demais órgãos convencionais.

O reflexo desse trabalho bem sucedido foi o cerne para criação da Lei nº 13.260, de 16 de março de 2016, popularmente conhecida como ‘Lei Anti-Terrorismo’. Teixeira (2015) faz uma referência:

> Cumpre ressaltar, ainda, que o crime cometido no ciberespaço possui classificações, sendo o crime virtual puro aquele que atenta o hardware e/ou software de um computador (parte física e parte virtual, respectivamente); crime virtual misto, no qual se utiliza internet para pratica de ilícitos, não com objetivo de danificar o hardware ou software e; crime

> virtual comum, onde a internet é usada apenas para realização de um fato típico já enquadrado no Código Penal.

Citando a respectiva lei, a punição para a prática de terrorismo cibernético é a seguinte:

> Artigo 2º, inciso IV da lei 13.260/2016:
> IV - sabotar o funcionamento ou apoderar-se, com violência, grave ameaça a pessoa ou **servindo-se de mecanismos cibernéticos**, do controle total ou parcial, ainda que de modo temporário, de meio de comunicação ou de transporte, de portos, aeroportos, estações ferroviárias ou rodoviárias, hospitais, casas de saúde, escolas, estádios esportivos, instalações públicas ou locais onde funcionem serviços públicos essenciais, instalações de geração ou transmissão de energia, instalações militares, instalações de exploração, refino e processamento de petróleo e gás e instituições bancárias e sua rede de atendimento. Pena - reclusão, de cinco a oito anos, e multa. (BRASIL, 2016).

A lei acima mencionada demonstra que se caso ocorra uma atividade de terrorismo cibernético, o autor, ou autores, não serão enquadrados como ameaça a segurança nacional.

4.3 NÚCLEOS DE CIBERDEFESA NO BRASIL

O Núcleo da Escola Nacional de Defesa Cibernética (NuENaDCiber), ativado por meio da portaria n° 002 do Comandante do Exército, de 02 de janeiro de 2015, a qual cria a Escola Nacional de Defesa Cibernética subordinada inicialmente ao CDCiber. Em consequência, a partir da data da publicação da referida portaria, a missão deste Núcleo é

> Fomentar e disseminar as capacitações necessárias à Defesa Cibernética, no âmbito da Defesa Nacional, bem como contribuir com as áreas de pesquisa, desenvolvimento, operação e gestão de Defesa Cibernética e para a melhoria da qualificação da mão de obra nacional para o setor. (BRASIL, 2015, p. 25)

Em virtude desse conjunto de ações, o atual Programa Estratégico de Defesa Cibernética (PEDC) incluiu o EB no restrito grupo de organizações, nacionais e internacionais, que possuem a capacidade de desenvolver medidas de proteção e mitigação de ataques no campo cibernético. O PEDC possui oito projetos estruturantes, dos quais é possível assinalar o Planejamento e Execução da

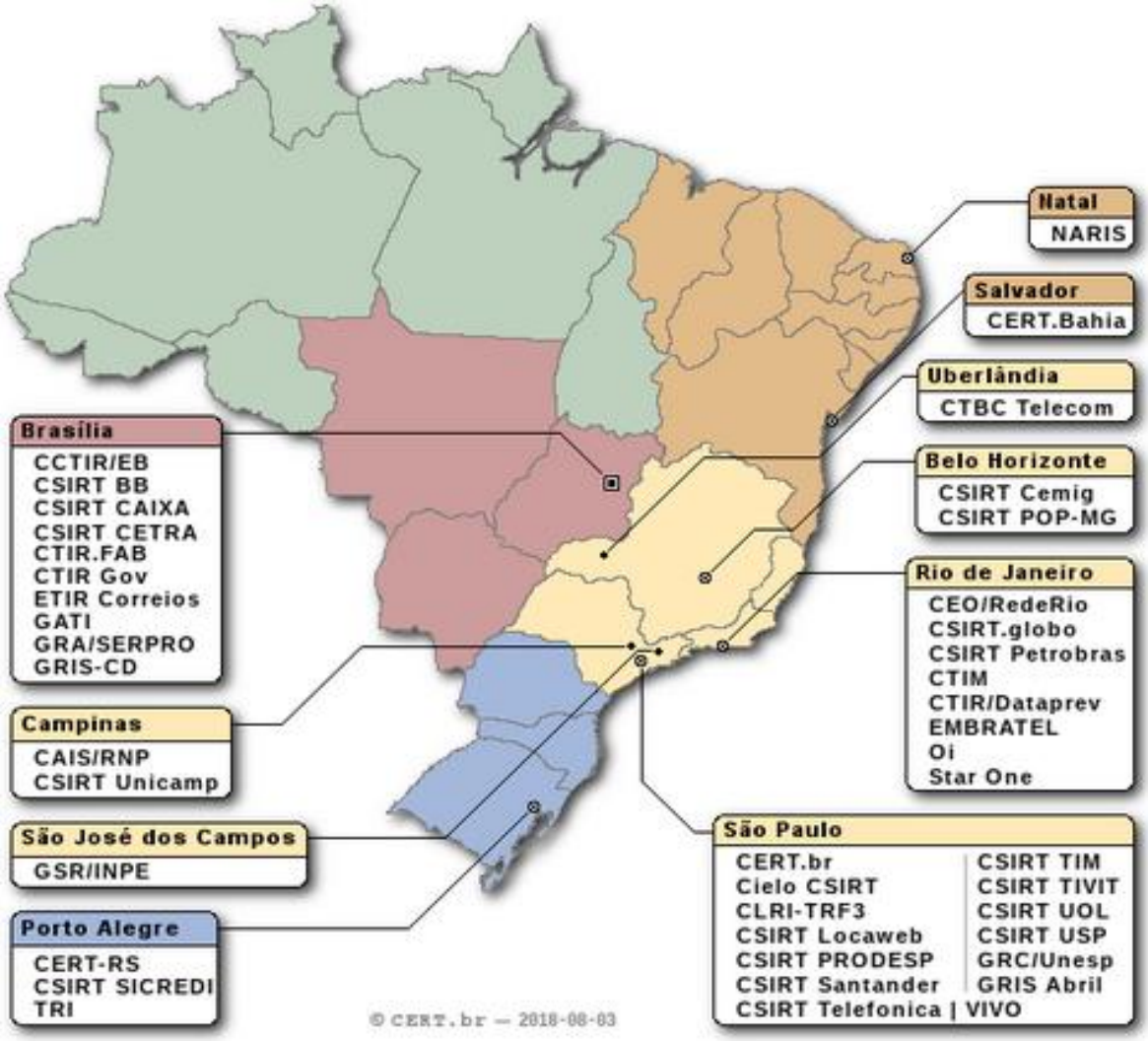
Segurança Cibernética, o de Estrutura de Pesquisa Científica na Área Cibernética e a Produção de doutrina específica para esse tipo de atividade, entre outros. Esses projetos estruturantes são conduzidos, atualmente, por Organizações Militares ligadas ao setor, como o Instituto Militar de Engenharia (IME), o Centro de Comunicações e Guerra Eletrônica do Exército, o Centro de Desenvolvimento de Sistemas do Exército, o Centro Tecnológico do Exército e o Centro de Inteligência do Exército.

4.4 GRUPOS DE RESPOSTA A INCIDENTES DE SEGURANÇA EM COMPUTADORES

À medida que a internet evoluía, ganhava normas e legislações para sua regulamentação no Brasil. Face à prevenção e ao controle de possíveis incidentes foram criados os Grupos de Resposta a Incidentes de Segurança em Computadores (CSIRTs). O CSIRT, apresentado na Figura 8, é responsável por receber, analisar e responder a incidentes de segurança em computadores envolvendo redes conectadas à internet Brasileira. Suas atribuições são:

- Trabalho de conscientização sobre os problemas de segurança;
- Auxílio ao estabelecimento de novos CSIRTs no Brasil;
- Desenvolvimento de documentação;
- Ponto central de contato para a internet no Brasil;
- Facilitação de ações entre redes envolvidas em incidentes;
- Trabalho colaborativo com outras entidades, como as polícias, provedores, *backbones* e setor financeiro.

Figura 8 – CSIRT no Brasil



Fonte: Cert.br (2018).

4.5 LIMITAÇÕES DA DEFESA CIBERNÉTICA

A observância no planejamento de ações de cibersegurança devem sempre colocar à luz das operações as limitações da Defesa Cibernética. O Manual MD31-M-07 (BRASIL, 2017) aponta quais são eles:

> São Limitações da defesa cibernética:
> a) limitada capacidade de identificação da origem de ataques cibernéticos;
> b) existência de vulnerabilidades nos sistemas computacionais;
> c) dificuldade de identificação de talentos humanos;
> d) grande vulnerabilidade a ações de oponentes com poder assimétrico;
> e) dificuldade de acompanhamento da evolução tecnológica na área cibernética; e
> f) possibilidade de ser surpreendido com base nas vulnerabilidades dos próprios sistemas de informação.

Do exposto a previsão de investimento e aperfeiçoamento, neste campo, é em médio prazo até 2020 e em longo prazo até 2030.

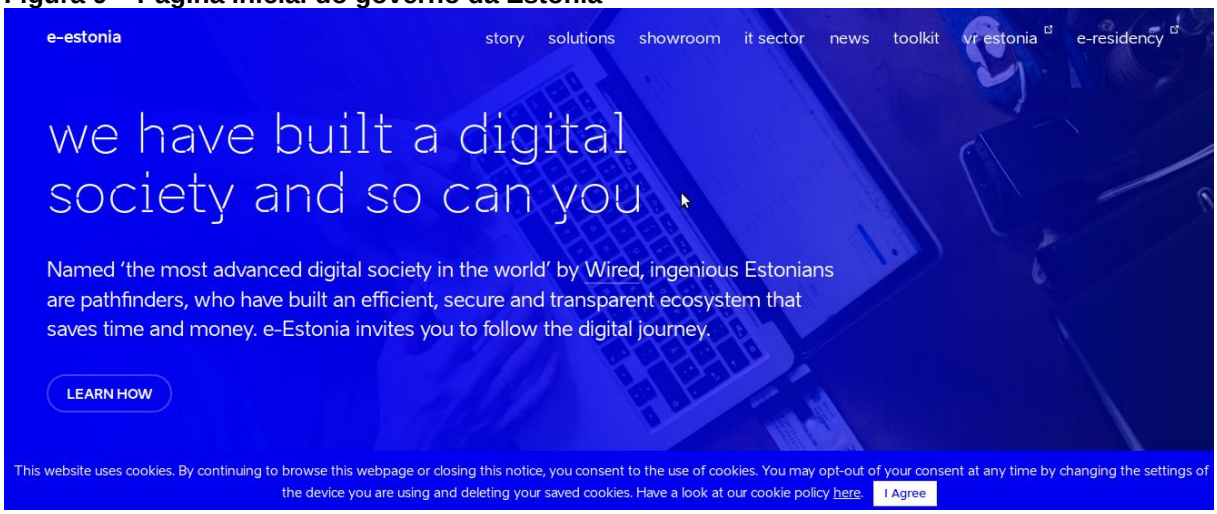
4.6 ATAQUES CIBERNÉTICOS

Este trabalho analisa três casos particulares – na área de transmissão de dados – que ocorreram na Estônia, Brasil e Irã, e que dividem a opinião a respeito da classificação, se foi ciberterrorismo ou ataque *hacker*. Este tipo de ataque refere-se ao acesso não autorizado que ocorre por meio das portas de entrada de uma conexão ou por intermédio de programas como vírus, *spywares, trojans*, etc.

4.6.1 O Caso da Estônia (2007)

A partir de 1997, a Estônia (Figura 9) se modernizou e adequou toda sua administração pública se tornando uma das primeiras nações a ter toda a governança na rede de dados. Fato que hoje corresponde a pelo menos 99% da sua administração pública.

Figura 9 – Página inicial do governo da Estônia



Fonte: Estônia (2018).

O início da causa do problema deve-se à remoção do Monumento aos Libertadores de Tallinn, apresentado na Figura 10, que homenageava o Exército russo contra os nazistas.

Figura 10 – Monumento aos libertadores de Tallinn

Fonte: McGuinness (2017).

Grande parte da população considerava que a estátua fazia uma referência à presença russa, a qual subjugou a Estônia durante a existência da União Soviética. Após a decisão de remover o referido monumento, se iniciou um ataque cibernético, conforme registrado na Folha de S. Paulo em sua edição do dia 18 de maio de 2007.

> Governo na Estônia é alvo de hackers. Sites oficiais e da mídia são invadidos e adulterados após realocação de monumento soviético, que desatou disputa com Rússia
>
> País báltico diz que chance de participação do governo russo na ação "não pode ser descartada"; cúpula entre Rússia e UE debate questão.
>
> A Estônia, país pioneiro na utilização da internet como plataforma de trabalho pelo governo, tem sido alvo de ataques praticados por hackers desde que se envolveu numa disputa com a Rússia causada pela realocação de um monumento em homenagem aos soldados soviéticos mortos na Segunda Guerra, há três semanas.
>
> Sites do governo, de partidos e da mídia da república báltica ficaram temporariamente fora do ar, em uma nação altamente dependente da internet. A Estônia foi o primeiro país do mundo a promover suas eleições online. O sistema bancário estoniano tem base na rede.
>
> Em um ataque a um site do Partido da Reforma, atualmente no poder, os hackers simularam um pedido de desculpas do primeiro-ministro aos russos pela realocação do monumento de uma praça central da capital do país para um cemitério afastado -ato que enfureceu a minoria russa na Estônia e a própria Rússia.
>
> A Otan (aliança militar ocidental), à qual a Estônia pertence desde 2004, enviou especialistas em ciberterrorismo a Tallinn para investigar e ajudar o país a recompor suas defesas eletrônicas. "Isso é uma operação de segurança, algo que estamos levando muito a sério", afirmou uma autoridade da Otan ao jornal britânico "The Guardian". "Não quero acusar

> ninguém, mas isso não é algo feito por poucos indivíduos." Apesar de não ter acusado a Rússia diretamente, a Chancelaria da Estônia publicou uma lista de endereços de IP de onde partiram as ações dos hackers, incluindo IPs pertencentes ao governo russo, e não descartou o envolvimento da Rússia. Além de endereços russos, o país registrou IPs do Brasil, Canadá, Vietnã e outros.
>
> "Os ciberataques vêm da Rússia. Não resta dúvida. É político", afirmou ao "Guardian" Merit Kopli, editor do jornal estoniano "Postimees".
>
> "Se você está insinuando que os ataques vieram da Rússia ou do governo russo, é uma acusação séria e precisa ser sustentada por provas", disse o embaixador russo em Bruxelas, Vladimir Chizhov, em resposta a uma pergunta do "Guardian".
>
> Os ataques de escala sem precedentes aos sites estonianos devem ser debatidos numa cúpula entre a Rússia e a União Européia, que começou ontem à noite em Samara (FSP, 2007).

Após esse ataque, os países ficaram em alerta devido à exposição da vulnerabilidade de transmissão de dados e o que uma invasão poderia acarretar nas áreas sensíveis atingindo o cotidiano da população. Conforme escreveu Marco Martins para a Revista Nação e Defesa (IDN, 2012, p. 32):

> Assumindo que o ciberespaço detém, por um lado, a capacidade de alocar um número infinito de páginas em linha sem custo adicional e, por outro lado, a possibilidade de desenvolver e de acompanhar os fluxos de informação em tempo mundial, pode considerar-se que representa uma ferramenta superior à de uma bomba nuclear dotada de capacidade de destruição global, não para o internauta comum, mas para aqueles que pretendam desenvolver ações criminosas. Estas novas ameaças emergentes que começam a operar para além do alcance das fronteiras físicas têm vindo a fomentar o incremento da segurança e a gestão de risco do Estado, nomeadamente no tocante ao sistema informático localizado nas estruturas vitais institucionais bem como a constituição de uma nova força não militar representada por civis que saibam operar em caso extremo de ciberguerra. Assim, presencia-se uma transformação da configuração dos setores da segurança e defesa que se projetam do Estado soberano para a realidade virtual, o que gera uma modificação da definição da política interna numa perspectiva internacional, dado que o ciberespaço não possui uma nacionalidade e/ou um território. Torna-se, por conseguinte, necessário, no sentido de proteger o Estado e respectivos cidadãos, o desenvolvimento de mecanismos de segurança e o reforço do papel do Estado enquanto entidade soberana e ator das relações internacionais.

4.6.2 Instalações Nucleares do Irã (2011)

Este caso, mundialmente explorado, é considerado um dos mais bem sucedidos já realizado, essa ação evitou, de forma direta, a possível construção de uma bomba nuclear iraniana (Figura 11), conforme noticiou o jornal O GLOBO em 17 de janeiro de 2011:

Vírus Stuxnet, que atacou usinas nucleares no Irã, foi criado em parceria por EUA e Israel.

Durante os dois últimos anos, segundo especialistas americanos militares e de inteligência, o complexo de Dimona, no deserto de Negev, em Israel, foi palco de testes secretos com o worm mais tarde conhecido como Stuxnet , para prejudicar os esforços do Irã no sentido de fabricar uma bomba nuclear. De acordo com o "New York Times", o projeto sigiloso foi uma parceria EUA-Israel, com alguma ajuda, consciente ou não, de Alemanha e Grã-Bretanha, e consistiu em por em funcionamento centrífugas nucleares virtualmente idênticas às localizadas em Natanz, no Irã, onde cientistas iranianos continuam tentando enriquecer urânio com finalidades bélicas.

Foi nessas centrífugas que foi testada a eficiência do worm Stuxnet, malware de computador que teria danificado cerca de um quinto das centrífugas iranianas, ajudando a atrasar - não destruir - a habilidade de Teerã em produzir suas primeiras armas nucleares.

De acordo com o "New York Times", o projeto sigiloso foi uma parceria EUA-Israel, com alguma ajuda, consciente ou não, de Alemanha e Grã-Bretanha, e consistiu em por em funcionamento centrífugas nucleares virtualmente idênticas às localizadas em Natanz, no Irã, onde cientistas iranianos continuam tentando enriquecer urânio com finalidades bélicas.

Foi nessas centrífugas que foi testada a eficiência do worm Stuxnet, malware de computador que teria danificado cerca de um quinto das centrífugas iranianas, ajudando a atrasar - não destruir - a habilidade de Teerã em produzir suas primeiras armas nucleares.

"Para testar o worm, é preciso conhecer as máquinas", disse ao "NYT" um especialista americano em inteligência nuclear. "A razão por que o worm foi efetivo é porque os israelenses testaram o software em condições reais".

O *malware Stuxnet* reconhecidamente foi a mais sofisticada ciber-arma já desenvolvida e aparentemente foi uma obra conjunta de diversos autores espalhados em vários continentes. No entanto, teria havido também cooperação de empresas da iniciativa privada, como a Siemens, que revelou a especialistas do Idaho National Laboratory, dos EUA, informações que permitiram identificar e explorar brechas de segurança bem escondidas em sistemas da empresa que foram exploradas pelo Stuxnet. O worm funcionava de duas maneiras principais. A primeira delas foi projetada para fazer com que as centrífugas iranianas começassem a girar loucamente fora de controle. A segunda forma inicialmente gravava dados telemétricos de uma típica operação normal das centrífugas nucleares, para depois reproduzir esse registro para os operadores dos equipamentos enquanto as máquinas, na verdade, as centrífugas estavam literalmente se desmantelando sob a ação do Stuxnet.

Alguns analistas americanos, porém, temem que essa iniciativa pioneira de ataque remoto a uma instalação iraniana seja a precursora de uma nova modalidade de guerra industrial à qual os próprios EUA seriam altamente vulneráveis (TEIXEIRA, 2011).

Figura 11 – Reator nuclear iraniano

Fonte: Cafétorah (2018).

4.6.3 Os ‘Apagões’ no Brasil

Segundo veiculado no programa americano “60 minutes”, a CIA havia alertado o governo brasileiro sobre um ataque *hacker* que afetaria a transmissão energética brasileira, no qual 90 milhões de pessoas ficaram sem energia elétrica, sendo esse considerado um dos piores incidentes na matriz energética brasileira. O Estadão, em 11 de novembro de 2009, publicou a seguinte matéria:

> Rede CBS diz que hackers causaram apagão de 2003. Fontes anônimas afirmando que os dois dias de apagão no setembro 2007, recentemente atribuído a hackers, foi na verdade resultado da negligência na manutenção de duas linhas de transmissão. Segundo o site, a informação tem como base relatório de agências do governo e outros órgãos que investigaram o incidente por mais de um ano. O programa 60 Minutes, da rede CBS, citou no domingo Espírito Santo foi provocado por hackers que atacaram a companhia que controla o sistema de energia. Segundo a rede, hackers também teriam sido responsáveis por outro pequeno apagão no Rio de Janeiro em janeiro de 2005. De acordo com algumas versões, eles estariam tentando extorquir dinheiro da empresa que controla o sistema de transmissão de energia.
>
> Funcionários do governo negaram a informação e a Furnas Centrais Elétricas disse ao Wired na segunda-feira que não tem conhecimento de que hackers agiram em seu sistema de transmissão.
>
> Segundo o site, a primeira explicação para o blecaute veio de Furnas dois dias após o incidente. A companhia disse que o apagão foi provocado por depósitos de fuligem na região do Espírito Santo. A Agência Nacional de Energia Elétrica multou Furnas em cerca de R$ 5,5 milhões pela má manutenção dos isolantes de alta voltagem nas torres de transmissão.
>
> Questionado se o blecaute de ontem poderia ter sido causado por hackers, o ministro das Minas e Energia, Edison Lobão, disse que, apesar dessas notícias já terem surgido, ele prefere acreditar que a causa tenha sido problemas atmosféricos. (ESTADÃO, 2009).

5 CONCLUSÃO

A revolução tecnológica elevou o espaço cibernético a uma nova condição nos assuntos relacionados à defesa e segurança. Tal espaço é um domínio global dentro da dimensão informacional do ambiente operacional que consiste em uma rede interdependente de infraestruturas de TIC e de dados, incluindo a internet, redes de telecomunicações, sistemas de computador, processadores embarcados e controladores.

A diversidade de pensamentos, ideias, ideologias, princípios, finalidades, transformam o ciberespaço em um terreno extremamente fértil para qualquer área de conhecimento. Este conhecimento pode ser difundido tanto para boas causas quanto para as más causas. A polaridade que novamente o mundo adentra, torna o compartilhamento da informação uma arma. Países estão se enfrentando diariamente em uma guerra por busca de dados ou tecnologia, em demonstrações de força em conseguir subtrair dados sensíveis, e até interferir no cotidiano de uma sociedade alterando os sistemas energéticos.

Se da mesma maneira que o Estado consegue perpetrar uma espécie de ‘Terrorismo de Estado Cibernético’, seja cerceando os meios de informações, ou usando a estrutura governamental para realizar ataques em alguma nação considerada inimiga, é provado que o mesmo tipo de ataque pode se voltar contra, através de grupos ou por atores isolados. Para muitos especialistas esta será a pior forma de guerra. Como exposto anteriormente, tradicionalmente o terrorismo não possui rosto. O terrorismo não dá ‘as caras’. Ele age através de células ou agentes infiltrados que normalmente são doutrinados, e existem aqueles que aderem a causa, simplesmente por concordar. Este tipo de agente, conhecido como ‘lobo solitário’, conforme seu conhecimento técnico, prática, acesso em níveis de segurança (se caso possuir), pode iniciar um ataque, ou uma alteração em algum sistema estruturado, que as autoridades ou órgãos de segurança podem considerar em primeira instância como um ataque *hacker*, desconhecendo seus reais propósitos.

O assunto ainda é controverso e de pouca difusão. O Brasil evoluiu muito nesta área nos últimos dez anos. A criação dos Centros de Defesa Cibernética e as ações interagências nos últimos grandes eventos que o país esteve envolvido diretamente, criou uma rede interligada (Figura 12), com apoio de órgãos civis e

OSP. A possibilidade de expansão em um limite longo até 2030, conforme prevê a END, possibilitará a concretização de medidas preventivas tanto para ataques cibernéticos e principalmente contra o ciberterrorismo.

Figura 12 – Eventos interagências de defesa cibernética

Fonte: Wallier (2014).

O artigo publicado por Gardini (2014), sintetiza essa ideia:

> A presença das organizações terroristas no ciberespaço e o problema que elas trazem para a segurança dos atores internacionais necessitam de atenção. Suas ações se realizam de diferentes formas, algumas facilmente identificáveis, e mobilizam discussões e curiosidade na sociedade. A pesquisa se inicia de forma a apresentar o ciberespaço, poder cibernético e a internet, conceitos básicos para entender como as organizações terroristas atuam nesse meio, quais são suas capacidades e a importância delas no contexto internacional atual. Assim, é possível perceber que o ciberespaço é um domínio cada vez mais presente na sociedade e, consequentemente, os atores internacionais utilizam-se do espaço cibernético como mais uma forma de exercer poder. Ao mesmo tempo em que é um novo campo de atuação para as questões internacionais, possui um alto número de usuários, baixos custos de entrada, capacidade de mudanças rápidas e condiciona a difusão de poder, o que acaba resultando na dificuldade de manter esse espaço totalmente seguro. Essa mesma difusão de poder que possibilita atores menores exercerem um papel maior no contexto internacional de forma positiva e com mais visibilidade, também possibilita a atuação de atores com intenções criminosas, os quais beneficiam-se das falhas nos sistemas de segurança. No caso das organizações terroristas, elas encontram no ciberespaço a possibilidade de divulgar e propagar seus ideais em uma escala mundial. O aperfeiçoamento dos grupos nas questões cibernéticas resulta na utilização do poder no ciberespaço de uma forma mais eficaz para seus objetivos, o que torna ainda mais importante a discussão desta questão para as relações internacionais, devido à ameaça que elas trazem para o cenário mundial. Assim, sendo a presença das organizações terroristas um fenômeno crescente no ciberespaço, o problema da pesquisa era indagar de que maneira estas organizações utilizam-se do espaço cibernético como ferramenta de atuação. Como resposta, foi identificada a atuação por meio de propaganda, financiamento, treinamento, planejamento, execução e ataques cibernéticos.

A visão global da evolução da internet foi sem dúvida um salto para a humanidade. A rapidez que a evolução dos meios físicos e o desenvolvimento de protocolos tornaram o mundo menor e a difusão do conhecimento uma forma rápida

e acessível. Dois mundos distintos, o bem e o mal, tramitam neste mundo invisível, o que faz com que a vigilância e a prevenção sejam as primeiras armas para evitar ações em que inocentes sejam vítimas.

No encerramento deste trabalho, se condensa o pensamento e a visão do EB, conforme descrito no Manual EB70-MC-10.232 (BRASIL, 2017):

> O surgimento de TIC avançadas facilitou a comunicação global, entre corporações, organizações extremistas violentas, e indivíduos. A possibilidade de compartilhar informações, em tempo real, de forma anônima e em segurança, é uma capacidade que pode, ao mesmo tempo, ser um trunfo para as forças militares, agências civis parceiras e aliados, como também tornar-se uma vulnerabilidade potencial a ser explorada por adversários. A obtenção, produção e difusão de informações relevantes, seletivas, oportunas e confiáveis têm relação direta com a qualidade e efetividade do processo decisório e com os meios e formas de lidar com a prevenção de ameaças, o gerenciamento de crises ou a solução de conflitos por parte dos instrumentos (diplomático, informacional, militar e econômico) do Poder Nacional. A informação tornou-se, assim, o componente primordial da Era do Conhecimento e uma poderosa ferramenta para influenciar, interromper ou afetar a capacidade do adversário de tomar e compartilhar as suas decisões.

REFERÊNCIAS

BAPTISTA, Ricardo Córdoba. **O que é ciberterrorismo**. Copyright© MyCyberSecurity, publicado em: 10 set. 2016. Disponível em: <https://www.mycybersecurity.com.br/glossario/ciberterrorismo/>. Acesso em: 20 out. 2018.

BARRETO **,** Eduardo Müssnich. **Terrorismo cibernético e cenários especulativos**. Revista Brasileira de Inteligência**.** Disponível em: <http://www.abin.gov.br/central-de-conteudos/publicacoes/>. Acesso em: 23 nov. 2018.

BASSO, Douglas Eduardo. **Análise de soluções UTM e ameaças digitais**. 2015. 70 f. Monografia (Especialização) – Programa de Pós-Graduação em Tecnologia, Universidade Tecnológica Federal do Paraná. Curitiba, 2015.

BRASIL. Casa Civil. **Lei nº 13.260, de 16 de março de 2016.** Regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Lei/L13260.htm>. Acesso em: 29 out. 2018.

BRASIL. **Livro verde:** Segurança cibernética no Brasil. Gabinete de Segurança Institucional. Secretaria Executiva. Departamento de Segurança da Informação e Comunicações. 2010. Disponível em: <http://dsic.planalto.gov.br/legislacao/1_Livro_Verde_SEG_CIBER.pdf>. Acesso em: 22 out. 2018.

BRASIL. **Centro de tratamento de incidentes de redes do governo**. Departamento de Segurança da Informação e Comunicações. Gabinete de Segurança Institucional. Estatística de Incidentes de Rede do Ano de 2017. 2017. Disponível em: <https://www.ctir.gov.br/arquivos/estatisticas/2017/Estatisticas_CTIR_Gov_Ano_2017.pdf>. Acesso em: 27 nov. 2018.

BRASIL. **Concepção operacional do sistema militar de defesa cibernética.** Ministério da Defesa. Brasília, DF: Ministério da Defesa, 2015.

BRASIL. **Doutrina militar de defesa cibernética. MD31-M-08.** Ministério da Defesa. Brasília, DF: Ministério da Defesa, 2014.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa (END)**. Disponível em: <https://www.defesa.gov.br/estado-e-defesa/estrategia-nacional-de-defesa>. Acesso em: 21 nov. 2018.

BRASIL. Ministério da Defesa. **Manual de abreviaturas, siglas, símbolos e convenções cartográficas das forças armadas.** MD33-M-02. Brasília, DF.

BRASIL. Ministério da Defesa. **Manual de política de segurança da informação para o sistema militar de comando e controle das forças armadas.** MD33-M-02. Brasília, DF, 2015.

BRASIL. Ministério da Defesa. **Portaria normativa nº 2.777/MD, de 27 de outubro de 2014,** Dispõe sobre a diretriz de implantação de medidas visando à potencialização da Defesa Cibernética Nacional. Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/19850/MD---PN-2777---Diretriz-de-Implantacao-de-Medidas-Visando-a-Potencializacao-da-Defesa-Cibernetica-Nacional/>. Acesso em: 25 nov. 2018.

BRASIL. **Segurança da informação e comunicações**. [20--]. Disponível em: <http://dsic.planalto.gov.br/assuntos/missao-do-dsic>. Acesso em: 26 nov. 2018.

CAFÉTORAH. **França contra Irã.** Copyright© Cafetorah, publicado em: 3 out. 2018. Disponível em: <https://www.cafetorah.com/franca-contra-ira/>. Acesso em: 26 nov. 2018.

CERT.BR. **Cartilha de segurança da internet**. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), publicado em: 03 mai. 2018. Disponível em: <http://cartilha.cert.br>. Acesso em: 30 out. 2018.

DINIZ, Kelly. **Ataques digitais cresceram 29% no Brasil em 2017.** Copyright© Grupo Minha, publicado em: 20 mar, 2018. Disponível em: <https://www.minhaoperadora.com.br/2018/03/ataques-digitais-cresceram-29-no-brasil-em-2017.html>. Acesso em: 18 out. 2018.

ESTADÃO. **Hackers causam apagão**. Copyright© Grupo Estado, publicado em: 11 nov. 2009. Disponível em: <https://www.estadao.com.br/noticias/geral,rede-cbs-diz-que-hackers-causaram-apagao-de-2007,464548>. Acesso em: 04 nov. 2018.

ESTÔNIA. **Página inicial do governo da Estônia**. 2018. Disponível em: <https://e-estonia.com/>. Acesso em: 15 out. 2018.

EUA. **The army universal task list.** Estados Unidos da América (EUA). Exército dos Estados Unidos. FM 7-15. Washington, DC: Army, 2012.
FORBES. **10 organizações terroristas mais ricas do mundo.** Copyright© Forbes Brasil, 2018. Disponível em: <https://forbes.uol.com.br/listas/2018/01/10-organizacoes-terroristas-mais-ricas-do-mundo/#foto10>. Acesso em: 24 out. 2018.

FSP. **Governo na Estônia é alvo de hackers.** Folha de S. Paulo (FSP), São Paulo, publicado em: 18 mai. 2007. Disponível em: <https://www1.folha.uol.com.br/fsp/mundo/ft1805200713.htm>. Acesso em: 21 nov. 2018.

GARDINI, Mayara Gabrielli. **Terrorismo no ciberespaço**: o poder cibernético como ferramenta de atuação de organizações terroristas. Fronteira, Belo Horizonte, v. 13, n. 25-26, p. 7-33, 2014. Disponível em: <http://periodicos.pucminas.br/index.php/fronteira/search?subject=Terrorismo>. Acesso em: 21 nov. 2018.

GRENZ, Stanley J.; SMITH, Jay T. **Dicionário de ética:** Mais de 300 Termos Definidos de Forma Clara e Concisa. Tradução de Alípio Correia de Franca Neto. São Paulo: Vida, 2005. Disponível em: <https://sites.google.com/view/sbgdicionariodefilosofia/cibern%C3%A9tica)>. Acesso em: 20 nov 2018.

HEZBOLLAH. **Página inicial Hezbollah**. 2018. Disponível em: <https://www.moqawama.org/>. Acesso em: 15 out. 2018.

HOEPERS, Cristine. **Privacidade e segurança de dados.** São Paulo: Vídeo, 2014. 21 slides, color. Disponível em: <https://www.cert.br/docs/palestras/certbr-forum-hbr2014.pdf>. Acesso em: 27 nov. 2018.

IDN. **Cibersegurança.** Instituto da Defesa Nacional (IDN), Revista Nação e Defesa, n. 133, Lisboa, Portugal, 2012. Disponível em: <https://www.idn.gov.pt/publicacoes/nacaodefesa/textointegral/NeD133.pdf>. Acesso em: 21 nov. 2018.

JIHAD. **Página inicial da Jihad Palestina**. 2018. Disponível em: <https://saraya.ps/>. Acesso em: 15 out. 2018.

MACHADO, Arthur Victor Baptista Carvalho Soares; et al. **Defesa cibernética comparada:** Um estudo do Brasil e da África do Sul. Artigo. 2017. Disponível em: <https://www.defesa.gov.br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/artigos/xiv_cadn/defesa_cibernetica_comparada_um_estudo_do_brasil_e_da_africa_do_sul.pdf>. Acesso em: 28 out. 2018.

MCGUINNESS, Damien. **How a cyber-attack transformed Estonia**. BBC News, publicado em: 27 abr. 2017. Disponível em: <https://www.bbc.com/news/39655415>. Acesso em: 25 out. 2018.

NUNES, Paulo Fernando Viegas. **Ciberterrorismo**: Aspectos de Segurança. Revista Militar, n. 2433, out. 2004, Portugal. Disponível em: <https://www.revistamilitar.pt/revista/2433>. Acesso em: 24 out. 2018.

PINTO, Marco Aurélio Gonçalves. **Teoria relativista do ciberterrorismo.** Dissertação para a obtenção do grau de Mestre em Guerra da Informação. Academia Militar. Lisboa, 2011. Disponível em: <https://comum.rcaap.pt/bitstream/10400.26/6826/1/Ciberterrorismo_tese_VersFinal.pdf>. Acesso em: 15 nov. 2018.

SALOMÃO, Cristiana Cota. **Arquitetura e cibernética**. Núcleo de Estudos de Habitares Interativos da USP. 2007. Disponível em: <http://www.nomads.usp.br/pesquisas/cultura_digital/arquitetura_e_cibernetica/textos%20linkados/artigo.pdf>. Acesso em: 19 nov. 2018.

SIBONI, Gabi; COHEN, Daniel; ROTBART, Aviv**. The threat of terrorist organizations in cyberspace**. Military and Strategic Affairs, v. 5, n. 3, dez. 2013. Disponível em: <http://www.inss.org.il/index.aspx?id=4300&researcherid=4916>. Acesso em: 19 nov. 2018.

SILVA, Willy Antunes Leal da. **A guerra eletrônica nas operações de informação em grandes eventos:** Copa do Mundo FIFA Brasil 2014 – Cidade-sede Recife/PE. 2017. 44 f. Trabalho de Conclusão de Curso (Especialização em Ciências Militares) - Curso Básico de Guerra Eletrônica, Centro de Instrução de Guerra Eletrônica, Brasília, 2017.

TEIXEIRA, Amandio. **Antes que eles acabem com o Brasil**. 100 Crônicas sobre os 13 – (ou partido, ou anos no poder). 1. ed. Clube de Autores (Edição Digital), 2015.

TEIXEIRA, Carlos Alberto. **Vírus stuxnet, que atacou usinas nucleares no Irã, foi criado em parceria por EUA e Israel.** 2011. Disponível em: <https://oglobo.globo.com/economia/virus-stuxnet-que-atacou-usinas-nucleares-no-ira-foi-criado-em-parceria-por-eua-israel-2836696>. Acesso em: 21 nov. 2018.

TROWBRIDGE, Alexander. **Jihadists on the move in Iraq with weapons, hashtags**. CBS News, 16 jun. 2014. Disponível em: <https://www.cbsnews.com/news/isis-jihadists-on-move-in-iraq-using-weapons-and-twitter-hashtags/>. Acesso em: 19 nov. 2018.

UNIÃO_EUROPEIA. **EUR-Lex - 32016D1136 – EM**. Decisão (PESC) 2016/1136 do Conselho, de 12 de julho de 2016, que atualiza a lista de pessoas, grupos e entidades a que se aplicam os artigos 2.°, 3.° e 4.° da Posição Comum 2001/931/PESC, relativa à aplicação de medidas específicas de combate ao terrorismo, e que revoga a Decisão (PESC) 2015/2430. Disponível em: < https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016D1136&from=PT>. Acesso em: 18 nov. 2018.

UNODC. **The use of the internet:** for terrorist purposes. United Nations Office on Drugs and Crime (UNODC). New York, 2012. Disponível em: <https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf>. Acesso em: 21 nov. 2018.

VISACRO, Alessandro. **Guerra irregular**: terrorismo, guerrilha e movimentos de resistência ao longo da história. São Paulo: Editora Contexto, 2009.

WALLIER, Eduardo. **CDCIBER:** Belém. Vídeo, 2014. 31 slides, color. Disponível em: <https://www.defesa.gov.br/arquivos/ensino_e_pesquisa/defesa_academia/cedn/viii_cedn/cibercidviiicedn.pdf>. Acesso em: 21 nov. 2018.