UNIVERSIDADE DE BRASÍLIA
INSTITUTO DE CIÊNCIAS HUMANAS
DEPARTAMENTO DE HISTÓRIA
PROGRAMA DE PÓS-GRADUAÇÃO EM HISTÓRIA

CIBERSEGURANÇA: UMA ANÁLISE DOS PRINCIPAIS CONFLITOS CIBERNÉTICOS GLOBAIS E SEUS IMPACTOS NO BRASIL

MICHEL GOMES NOGUEIRA

ORIENTADOR: PROFESSOR DOUTOR VIRGÍLIO CAIXETA ARRAES

BRASÍLIA - 2024

UNIVERSIDADE DE BRASÍLIA
INSTITUTO DE CIÊNCIAS HUMANAS
DEPARTAMENTO DE HISTÓRIA
PROGRAMA DE PÓS-GRADUAÇÃO EM HISTÓRIA

CIBERSEGURANÇA: UMA ANÁLISE DOS PRINCIPAIS CONFLITOS CIBERNÉTICOS GLOBAIS E SEUS IMPACTOS NO BRASIL

MICHEL GOMES NOGUEIRA

Tese apresentada ao Programa de Pós-graduação em História da Universidade de Brasília como requisito parcial para a obtenção do grau de Doutor em História

Área de concentração: Sociedade, Política e Cultura

Linha de Pesquisa: Política, Instituições e Relações de Poder

Orientador: Prof. Dr. Virgílio Caixeta Arraes

BRASÍLIA - 2024

À minha preciosa esposa, **Nara**, ao meu
amado filho, **Pedro**, ao meu querido pai,
Altair e à minha querida **mãe**, Virginia.
Alicerces da minha vida, presentes de Deus.
Amor sem fim.

AGRADECIMENTOS

Deus Pai, sem Ti nada seria possível.

Ao meu orientador Professor Dr. Virgilio Caixeta Arraes, pelo conhecimento, compartilhamento e amizade.

À minha família, Nara Fabiana da Cunha e Pedro da Cunha Nogueira, por todo apoio e paciência.

Aos meus pais Altair Gomes Nogueira e Virginia da Silva Nogueira, por me ensinarem a amar a leitura.

Ao amigo Satiro Lazaro da Cunha (in memoriam), pelas histórias cativantes.
À querida Dalmina Moreira da Cunha, por todo carinho.

Gratidão por tudo!

O que é já foi, e o que será também já foi anteriormente;

Deus investigará o passado.

Eclesiastes 3:15 NVI

RESUMO

CIBERSEGURANÇA: UMA ANÁLISE DOS PRINCIPAIS CONFLITOS CIBERNÉTICOS GLOBAIS E SEUS IMPACTOS NO BRASIL

A cibersegurança tornou-se uma questão premente na era da informação, com incidentes que se tornam cada vez mais frequentes e sofisticados. A pesquisa busca analisar alguns dos principais conflitos cibernéticos mundiais, tais como os ocorridos na Estônia (2007), Geórgia (2008), Stuxnet (2010) e os supostos ataques às concessionárias de energia elétrica no Brasil nos anos de 2005, 2007 e 2009. O estudo correlaciona esses ataques a alguns dos grandes eventos sediados pelo Brasil nesse início de século: a Conferência Rio +20 (2012), Copa das Confederações (2013), Jornada Mundial da Juventude (2013), Copa de Mundo (2014), Jogos Olímpicos e Paralímpicos (2016). Parte do legado estabelecido por esses eventos internacionais e nacionais demonstraram a necessidade de o governo brasileiro estabelecer diretrizes e aperfeiçoar os dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos e, se for o caso, que permitam seu pronto restabelecimento. Uma ação de defesa tendo como base as leis internacionais ou as nacionais poderia ser uma decisão coerente, assim como uma resposta militarizada, com o uso até mesmo de armamentos de guerra cinética. Essa possibilidade encontra respaldo na história recente do ambiente cibernético, pois são diversos fatores envolvidos que precisariam ser analisados para uma tratativa efetiva de um conflito cibernético entre nações que tenham como alvo o funcionamento do sistema financeiro, a matriz energética, os meios de transportes, as telecomunicações, a rede de dados: além de impor risco de morte e a falência da atuação orgânica de toda uma sociedade. Para suporte a toda essa nova conjuntura, o Brasil estabeleceu em 2014 a Doutrina Militar de Defesa Cibernética cuja finalidade é unificar o pensamento no âmbito do Ministério da Defesa (MD), e apoiar uma atuação conjunta das Forças Armadas (FA) na defesa do Brasil no espaço cibernético. Muito desse arcabouço normativo é avaliado na tese de pesquisa, em conjunto com os estudos de casos apresentados e as medidas adotadas para a defesa cibernética ao sediar grandes eventos internacionais, a fim de detectar as possíveis forças e fraquezas da segurança cibernética brasileira.

Palavras-chaves: Cibersegurança, Conflitos Cibernéticos, Tecnologia da Informação e Comunicação (TIC).

SUMMARY

CYBER SECURITY: AN ANALYSIS OF THE MAIN GLOBAL CYBER CONFLICTS AND THEIR IMPACTS IN BRAZIL

Cybersecurity has become a pressing issue in the information age, with incidents becoming increasingly frequent and sophisticated. The research seeks to analyze some of the main global cyber conflicts, such as those that occurred in Estonia (2007), Georgia (2008), Stuxnet (2010) and the alleged attacks on electricity utilities in Brazil in 2005, 2007 and 2009. The study correlates these attacks with some of the major events hosted by Brazil at the beginning of this century: the Rio +20 Conference (2012), Confederations Cup (2013), World Youth Day (2013), World Cup (2014), Olympic Games Olympic and Paralympic Games (2016). Part of the legacy established by these international and national events demonstrated the need for the Brazilian government to establish guidelines and improve security devices and procedures that reduce the vulnerability of systems related to the National Defense against cyber attacks and, if applicable, that allow their prompt recovery. A defense action based on international or national laws could be a coherent decision, as could a militarized response, with even the use of kinetic warfare weapons. This possibility finds support in the recent history of the cyber environment, as there are several factors involved that would need to be analyzed for an effective handling of a cyber conflict between nations that target the functionality of the financial system, the energy matrix, the means of transport, the telecommunications, the data network: in addition to imposing a risk of death and the failure of the organic performance of an entire society. To support this new situation, Brazil established in 2014 the Military Doctrine of Cyber Defense whose purpose is to unify thinking within the scope of the Ministry of Defense (MD), and support joint action by the Armed Forces (FA) in the defense of Brazil in cyberspace. Much of this normative framework is evaluated in the research thesis, together with the case studies presented and the measures adopted for cyber defense when hosting major international events, in order to detect the possible strengths and weaknesses of Brazilian cyber security.

Keywords: Cybersecurity, Cyber Conflicts, Information and Communication Technology (ICT).

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE TABELAS

ABREVIATURAS, SIGLAS E ACRÔNIMOS

ABIN	Agência Brasileira de Inteligência
ACE	Automatic Computing Engine
ACEM	Automated Continuous Endpoint Monitoring
ACSL	Analog Computer Simulation Language
AMPATH	Americas Path Network
ARPA	Advanced Research Projects Agency
ATM	Asynchronous Transfer Mode
BNDE	Banco Nacional de Desenvolvimento Econômico
CAPRE	Comissão de Coordenação das Atividades de Processamento Eletrônico
CCPR	Casa Civil da Presidência da República
CDCiber	Centro de Defesa Cibernética
CEI	Comunidade de Estados Independentes
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CESI	Comitê Executivo de Segurança Integrada
CGI	Comitê Gestor da Internet
CIA	Central Intelligence Agency
CIS	Center for Internet Security
CLARA	Cooperação Latino-Americana de Redes Avançadas
CMA	Coordenação de defesa de área
CML	Comando Militar do Leste
CNA	Computer Network Attack
CNCIBER	Comitê Nacional de Cibersegurança
CNCiber	Comitê Nacional de Cibersegurança
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Computer Network Operations
COB	Comitê Olímpico Brasileiro
COBRA	Computadores e Sistemas Brasileiros
COI	Comitê Olímpico Internacional
ComDCiber	Comando de Defesa Cibernética
COMLURB	Companhia Municipal de Limpeza Urbana
CPI	Comissão Parlamentar de Inquérito
CSIRT	Computer Security Incident Response Team
CSMP	Continuous System Modeling Program
CSN	Conselho de Segurança Nacional
CTIR Gov	Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo
DARPA	Defense Advanced Research Projects Agency
DDoS	Distributed Denial-of-Service
DEPIN	Departamento de Política de Informática e Automação
DIGIBRÁS	Empresa Digital Brasileira S.A
DIH	Direito Internacional Humanitário
DoD	Departamento de Defesa norte-americano
DoS	Denial-of-Service
DSI/GSI	Departamento de Segurança da Informação do Gabinete de Segurança Institucional

DSR	Digital Silk Road
E-Ciber	Estratégia Nacional de Segurança Cibernética
EE	Equipamentos eletrônicos
EMCFA	Estado-Maior Conjunto das Forças Armadas
ENaDCiber	Escola Nacional de Defesa Cibernética
END	Estratégia Nacional de Defesa
ENIAC	Electronic Numerical Integrator and Computer
ETIRs	Equipes de tratamento de incidentes de redes
EUA	Estados Unidos da América
EW	Eletronic Warfare
FCCN	Fundação para a Computação Científica Nacional
FEP	Fuel Enrichment Plant
FHC	Fernando Henrique Cardoso
FR	Frame Relay
GEACE	Grupo Executivo para Aplicação de Computadores Eletrônicos
GGE	Group of Governmental Experts
GTE	Grupo de Trabalho Especial
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
IA	Inteligência Artificial
IBASE	Instituto Brasileiro de Análises Sociais e Econômicas
ICCyber	Conferência Internacional de Perícias em Crimes Cibernéticos
IME	Instituto Militar de Engenharia
IMP	Interface Message Processor
IP	Internet Protocol
IPC	International Paralympic Committee
IPTO	Information Processing Techniques Office
IS	Islamic State
ITA	Instituto Tecnológico da Aeronáutica
ITU-T	International Telecommunication Union - Telecomunication
JMJ	Jornada Mundial da Juventude
LBDN	Livro Branco de Defesa
LSD	Laboratório de Sistemas Digitais
MCT	Ministério de Ciência e Tecnologia
MD	Ministério da Defesa
MILDEC	Military Deception
MIT	Massachusetts Institute of Technology
MJ	Ministério da Justiça
MPL	Movimento Passe Livre
NASA	National Aeronautics and Space Administration
NPL	National Physical Laboratory
NSA	National Security Agency
NuComDCiber	Núcleo do Comando de Defesa Cibernética
NuENaDCiber	Núcleo da Escola Nacional de Defesa Cibernética
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
OEWG	Open Ended Working Group
OMS	Organização Mundial da Saúde
OMS	Organização Mundial de Saúde
ONS	Operador Nacional do Sistema Elétrico
ONU	Organização da Nações Unidas

OPSEC	Operation Security
OSP	Órgãos de Segurança Pública
OTAN	Organização do Tratado do Atlântico Norte
P&D	Pesquisa e Desenvolvimento
PCC	Partido Comunista Chinês
PIB	Produto Interno Bruto
PLC	Programmable Logic Controller
PNCiber	Política Nacional de Cibersegurança
PND	Política Nacional de Defesa
PND	Plano Nacional de Desenvolvimento
PNI	Política Nacional de Informática
PSYOP	Psychological Operations
PT	Partido dos Trabalhadores
RCTS	Rede Ciência, Tecnologia e Sociedade
RFID	Radio-Frequency Identification
RNP	Rede Nacional de Ensino e Pesquisa
SCADA	Supervisory Control and Data Acquisition
SCT	Secretaria de Ciência e Tecnologia da Presidência da República
SDH	Synchronous digital hierarchy
SEGCIBER	Segurança Cibernética
SEI	Secretaria Especial de Informática
SERPRO	Serviço Federal de Processamento de Dados
SESGE	Secretaria Extraordinária de Segurança para Grandes Eventos
SIGINT	Signals Intelligence
SISBIN	Sistema Brasileiro de Inteligência
SMDC	Sistema Militar de Defesa Cibernética
SMTP	Simple Mail Transfer Protocol
SRI	Stanford Research Institute
TCP	Transmission Control Protocol
TCU	Tribunal de Contas da União
TIC	Tecnologia da Informação e Comunicação
TOC	Technology Operational Centre
UCLA	Universidade da Califórnia em Los Angeles
UCSB	Universidade Californiana de Santa Bárbara
UEM	Universidade Estadual de Maringá
UIT	União Internacional das Telecomunicações
UIT	União Internacional de Telecomunicações
UNIVAC	Universal Automatic Calculator
URSS	União das Repúblicas Socialistas Soviéticas
US-CCU	U.S. Cyber Consequences Unit
UTI	Unidade de Tratamento Intensivo
WTC	World Trade Center
WWW	World Wide Web

SUMÁRIO

Introdução

O primeiro ano do século XXI foi marcado pelos atentados terroristas do dia 11 de setembro de 2001, quando os Estados Unidos sofreram o maior ataque em seu território desde o bombardeio japonês à base de Pearl Harbor (no Havaí, em 1941) durante a Segunda Guerra Mundial.

Na manhã daquela terça-feira de setembro, o mundo assistiu atônito pelos canais de televisão as imagens do impacto de dois aviões sequestrados na costa leste do país que colidiram contra as torres gêmeas do World Trade Center (WTC), na ilha de Manhattan, em Nova York. Pouco tempo depois ambas as torres desabaram, depois que suas estruturas terem sido abaladas pelo fogo provocado pelos combustíveis das aeronaves.

Ainda tiveram dois outros aviões sequestrados, um que se chocou com o Pentágono (sede do Departamento de Defesa dos Estados Unidos), em Washinghton D.C, e o outro que não atingiu o alvo pretendido pois os próprios passageiros lutaram contra os sequestradores e a aeronave acabou caindo numa área desabitada no Estado da Pensilvânia.

O 11 de Setembro contabilizou a morte de 2.977 pessoas, além dos 19 sequestradores dos aviões, considerado o ataque terrorista com o maior número de mortos da história, além de ter sido uma tragédia que mudou, em vários aspectos, os rumos do mundo (BBC, 2021a).

Em 2023, um ataque cibernético paralisou 16 hospitais e mais de 160 clínicas e centros de saúde em quatro estados americanos. O ataque afetou o funcionamento da rede hospitalar da *Prospect Medical Holdings* e interrompeu serviços de emergência e suspensão de cirurgias eletivas em diferentes unidades. A empresa responsável pela administração da rede de hospitais detalhou ter sido vítima de um ataque cibernético, que impossibilitou o funcionamento dos sistemas. A identificação do incidente de segurança da informação fez com a rede hospitalar desligasse os seus sistemas de tecnologia (DEMARTINI, 2023).

No hospital Waterbury, centro de referência da quinta maior cidade do estado americano do Connecticut, atendimentos de urgência passaram a ser realizados com prontuários de papel até a restauração dos sistemas. Em outubro de 2022, um ataque semelhante foi realizado a rede hospitalar da *CommonSpirit Health*, a maior organização

do setor americano. Os sistemas da rede ficaram indisponíveis e houve o vazamento de dados de mais de 623 mil pacientes e acompanhantes, incluindo prontuários e outras informações sensíveis (DEMARTINI, 2023).

Tanto o ataque terrorista do 11 de setembro de 2021 quanto o ataque cibernético aos hospitais americanos em 2023 foram distintos na forma de execução, um aconteceu pela colisão de aeronaves a instalações físicas, com a perda de milhares de vida, o outro utilizou-se dos meios tecnológicos para danificar sistemas digitais e paralisar o atendimento de milhares de pacientes que aguardavam atendimento médico. No entanto, ambos tiveram algo em comum: a perda definitiva ou temporária de informações.

Muitas empresas que atuavam no WTC tinham cópias de segurança dos seus sistemas, mais conhecido em inglês como *backup,* o problema é que estavam localizadas em ambas as torres ou nas proximidades em áreas afetadas pela destruição. Ou seja, quando uma torre foi atacada, não se pensou que a outra também poderia ser. O sistema de cópia de segurança foi destruído quando ambas as torres desmoronaram. Algumas dessas empresas, além de perderem vidas humanas, perderam também todas as suas informações, que afetaram não só os seus clientes que dependiam desses dados, como também a continuidade de seus negócios. Mais da metade das pequenas e médias empresas afetadas pelo 11 de setembro fecharam as portas porque perderam tudo e não conseguiram se reestruturar novamente (SPANIOL, 2015).

O ataque cibernético aos hospitais americanos também refletiu na vida de milhares de americanos pelo fato de que as informações também não se encontravam mais disponíveis, nesse caso, a indisponibilidade, diferentemente de algumas empresas localizadas no WTC, foi temporária, pois foi necessário restaurar todos os sistemas para que a situação voltasse a normalidade.

A informação sempre foi um ativo importante para pessoas físicas ou jurídicas, quer sejam simples cidadãos, pequenas, médias ou grandes empresas, governos, instituições públicas, privadas, setores logísticos e produtivos, ambiente acadêmico, etc. A migração da informação do papel para o meio digital é algo irreversível; a evolução da tecnologia da informação é algo sem precedentes. Cada vez mais o ser humano é depende de informações digitais para realizar as mínimas atividades em seu dia a dia. A história do século XXI é de um mundo que gira ao redor de um eixo cibernético.

Mas, para se pensar em uma sociedade informatizada, faz-se necessário passar pelo grifo da cibersegurança, também conhecida como segurança cibernética, com intuito de proteger os dados em meio digital, dispositivos (hardware) e recursos (software) contra ameaças cibernéticas, garantindo a confidencialidade, integridade e disponibilidade das informações.

De acordo com o Setor de Normatização das Telecomunicações da União Internacional de Telecomunicações da ONU, conhecido pelo acrônimo inglês ITU-T, cibersegurança é definido como:

> Conjunto de ferramentas, políticas, conceitos de segurança, diretrizes, abordagens de gestão de risco, ações, treinamentos, melhores práticas, garantias e tecnologias que podem ser utilizadas para proteger os ativos do ambiente cibernético, da organização e dos usuários. Os ativos da organização e do usuário incluem dispositivos de computação conectados, pessoal, infraestrutura, aplicações, serviços, sistemas de telecomunicações e a totalidade de informações transmitidas e/ou armazenadas no ambiente cibernético. A cibersegurança busca garantir o cumprimento e a manutenção das propriedades de segurança dos ativos da organização e dos usuários contra riscos relevantes à segurança encontrados no ambiente cibernético. Os objetivos gerais de segurança compreendem o seguinte: disponibilidade, confidencialidade e integridade, que pode incluir autenticidade e não repúdio (ITU-T, 2008, p. 2–3).

Para o governo federal, a cibersegurança ou a segurança cibernética refere-se à prática de proteger sistemas, redes e programas de ataques digitais, que geralmente visam a acessar, alterar ou destruir informações sensíveis e extorquir dinheiro de usuários ou interromper processos empresariais (BRASIL, 2023a). Segundo a empresa privada internacional de segurança virtual, Kaspersky, a cibersegurança pode ser chamada de segurança da tecnologia da informação ou segurança de informações eletrônicas.

O termo é aplicável a uma variedade de contextos, desde negócios até computação móvel, e pode ser dividida em algumas categorias comuns: segurança de rede, segurança de aplicativos, segurança de informações, segurança operacional, recuperação de desastres e continuidade de negócios e educação do usuário final. Além do mais, abrange áreas como criptografia, autenticação, prevenção contra intrusões, análise de dados, inteligência artificial e muito mais (KASPERSKY, 2024a).

À medida que a tecnologia da informação se torna cada vez mais integrada em todos os aspectos da nossa sociedade, aumenta-se o risco de eventos de grande escala ou de grandes consequências que possam causar danos ou perturbar serviços dos quais dependem a nossa economia e a vida quotidiana dos cidadãos.

Ocorre que os ataques cibernéticos não esperam que as sociedades estejam preparadas para enfrentá-los, ao contrário, são mais eficazes quando os critérios de segurança são considerados fracos e insuficientes. Por isso, os conflitos cibernéticos se tornaram rapidamente um assunto de interesse global, pois afetam a todos de igual modo, sejam pessoas, empresas, governos ou forças de segurança, ou seja, tudo que se move no espaço cibernético está suscetível a confrontar uma força “oculta”.

Não estão limitados a fronteiras territoriais, não existe um campo de batalha definido, não estão necessariamente sujeitos a governos, são de difícil atribuição e responsabilização, o tempo entre o lançamento de um ataque e seus efeitos são dificilmente mensuráveis. A imprevisibilidade de um ataque cibernético, caso seus efeitos se estendam a diversos setores de uma sociedade e evoluam para um espectro de grande escala, poderá alterar o equilíbrio militar mundial, bem como alterar as relações políticas, sociais e econômicas de uma nação.

A história registrou em um tempo recente ataques cibernéticos emblemáticos como o ocorrido na Estônia em 2007, a invasão russa em território georgiano em 2008 precedido também de um ataque cibernético de grande escala e a destruição de milhares de centrífugas de enriquecimento de urânio no Irã por um vírus de computador conhecido como Stuxnet em 2010.

Preocupado com a alta sofisticação dos ataques cibernéticos e os seus efeitos catastróficos, o governo brasileiro buscou instrumentalizar-se com objetivo de aprimorar a sua defesa cibernética, principalmente quando foi escolhido para sediar grandes eventos mundiais que ocorreram no país, como a Conferência Rio +20 (2012), Copa das Confederações (2013), Jornada Mundial da Juventude (2013), Copa do Mundo (2014), Jogos Olímpicos e Paralímpicos (2016).

Em dezembro de 2023, o governo brasileiro criou o Comitê Nacional de Cibersegurança (CNCIBER) para ser responsável por avaliar e propor medidas para aumentar a segurança cibernética no Brasil. O comitê será composto por 25 membros, com representantes do governo, sociedade civil, setor privado e instituições tecnológicas. Uma de suas atribuições será a formulação de propostas para prevenir, detectar e combater ataques de intrusos cibernéticos contra a infraestrutura crítica nacional e os serviços essenciais, como o sistema financeiro, o controle de tráfego aéreo e a distribuição de energia elétrica.

Nesse arcabouço apresentado, a ideia que se tem quanto ao papel do historiador é a de compreender e explicar os eventos, processos e mudanças que ocorreram em diferentes sociedades e culturas no passado e seus impactos e relevância para a época atual.

Como diria Eric Hobsbawm (1995): “a principal tarefa do historiador não é julgar, mas compreender, mesmo o que temos mais dificuldade para compreender. O que dificulta a compreensão, no entanto, não seriam apenas as convicções apaixonadas, mas também a experiência histórica que as formou”. Se a história fosse julgada incapaz de outros serviços, para Marc Bloc, “ela entretém”, seria como um passatempo, algo que mais lhe agrada e descobrir a sua ciência e a ela dedicar é propriamente o que se chama vocação (BLOCH, 2001, p.43).

Jacques Le Goff transcreve que a necessidade do historiador de misturar relato e explicação fizeram da história um gênero literário, uma arte ao mesmo tempo que uma ciência, mas o crescente tecnicismo da ciência histórica a partir do século XX tornou mais difícil para o historiador parecer também um escritor, mesmo assim existe sempre uma “escritura da história” (LE GOFF, 1990, p.13).

Nesse sentido, escrever sobre a história digital pode ser entendido como a busca do autor por uma nova compreensão do mundo através das lentes que permeiam o espaço cibernético. É investigar o que não é muito conhecido para produzir novas reflexões no contexto da ciência histórica. Deseja-se que o trabalho apresentado possa “entreter” mesmo que o “abuso” ou demasia de termos técnicos e tecnológicos não sejam de simples leitura e compreensão.

Para realizar uma investigação, o historiador pode se valer do uso de diferentes tipos de fontes de informação, sejam documentos oficiais, cartas, fotografias, objetos, registros orais. A Internet possibilitou a digitalização de muitos desses documentos, sendo que muitos deles já nasceram digitalizados.

Com o advento da pandemia do coronavírus ou COVID-19 (SARS-CoV-2), que teve o seu início no dia 11 de março de 2020 e o seu fim em 5 de maio de 2023, conforme determinação da Organização Mundial da Saúde – OMS (OPAS, 2023), muitos dos estudos e pesquisas históricas que deveriam ter sido realizadas em ambiente externos, como acervos de documentos físicos, bibliotecas, arquivos, etc, ficaram suspensos boa parte desse período para fins de contenção da transmissão da doença. O que permitiu a

continuidade dos trabalhos foram exatamente as consultas realizadas em acervos ou repositórios digitais acessados via sites acadêmicos e de busca pela Internet.

Ao analisar os documentos digitais o autor considerou o contexto social, econômico e cultural dos fatos históricos relatados e os correlacionou ao conhecimento científico sobre o tema. Na intenção de se encontrar uma forma de contextualizar o problema relatado desta pesquisa e formatá-lo para uma compreensão clara, precisa e concisa, o autor entendeu por bem explicá-lo por meio do analogismo.

Dito isso, imagine a situação de uma casa, onde ali more um grupo de pessoas. Uma de suas preocupações é manter a moradia segura e protegida contra possíveis invasores. Com intuito de aumentar a proteção do local, o grupo decide por adquirir diversos itens de segurança disponíveis no mercado, como instalação de rede eletrificada, monitoramento por vídeo, controle de entrada e saída, etc.

Transportando-se desse ambiente micro para um cenário macro, o limite territorial da casa se compararia ao espaço cibernético brasileiro, os utensílios utilizados na casa às informações digitais; os dispositivos de segurança à defesa cibernética brasileira. Imaginemos que exista um invasor nas redondezas da casa cuja pretensão seja de furtar os seus bens, só que a única forma disso acontecer seria por meio de vulnerabilidades encontradas, por uma porta aberta, um sistema de alarme que não foi ativado, uma senha fraca para abertura de uma porta com fechadura eletrônica, etc.

Enfim, uma analogia simples para demonstrar um problema complexo, ou seja, mesmo com todo o investimento realizado, a casa ainda poderia continuar vulnerável a ataques, da mesma forma um país por mais que tenha investido em tecnologia, normativos e treinamento para aprimorar a sua segurança cibernética, ainda assim não estaria totalmente protegida. Sim, é fato que não existe 100% de segurança no mundo virtual e nenhuma empresa de cibersegurança venderia uma solução com essa proposta.

No mundo físico é mais fácil identificar o invasor, ele é visível e passível de ser contido, no mundo digital, o inimigo é invisível, ele poderá realizar um ataque cibernético de qualquer região do planeta a qualquer momento e até mesmo dentro do seu próprio país, sem que se tenha total certeza de quem realmente ele é.

De acordo com um relatório da Trend Micro, empresa de soluções em cibersegurança, o Brasil é o segundo país mais vulnerável a ataques cibernéticos, atrás

apenas dos Estados Unidos. O país teve bilhões de ameaças bloqueadas no primeiro semestre de 2023. A Trend Micro relatou que nesse período bloqueou cerca de 85,6 bilhões de ameaças em todo o mundo, um valor que já é 59% do total registrado em 2022. Estados Unidos, Brasil e Índia são os principais alvos, em ordem de incidência (SILVA, 2023)

O Brasil é o principal alvo de ciberataque na América Latina e segundo Nalin (2023) esta é uma realidade da região há quase uma década. No segundo semestre de 2022, o país sofreu um aumento de 19% no número de tentativas de ataques cibernéticos comparado ao primeiro semestre. Um aumento considerado superior ao observado na média mundial, que foi de 13% no período.

Segundo especialistas em segurança cibernética, o Brasil está na mira dos cibercriminosos devido ao avanço da tecnologia e a popularização dos serviços bancários pela Internet e celular, acrescente-se o fato de que cada vez mais o setor comercial tem migrado para as compras digitais. Um relatório da Kaspersky apontou que o Brasil é o país mais afetado por golpes financeiros na América Latina, seguido por México, Peru e Colômbia (LORENZO, 2024).

A proposta é que esta pesquisa trate do problema de se identificar e coletar evidências em fontes históricas digitais que tratem do desenvolvimento e avanço do espaço cibernético e de seus conflitos, que resultaram em achados que foram possíveis pontos de vulnerabilidades da defesa cibernética brasileira e a forma como foram mitigados no período dos grandes eventos realizados no país.

Nesse contexto de historiografia digital, utilizou-se da visão de Chartier (2002, p. 105) que diagnosticou que o século XX é constituída por uma “civilização da tela, do triunfo das imagens e da comunicação eletrônica”. Ele trata da antiga oposição que destaca de um lado o livro, a escrita, a leitura e, de outro, a tela e a imagem como novo suporte para a cultura escrita e uma nova forma para o livro.

Segundo Pires e Amorim (2021, p. 2) o uso de ferramentas digitais no campo das humanidades tem sido imprescindível e as novas formas de pesquisa têm impactado fortemente a produção de conhecimento histórico no tempo presente e exercem fortes influências nas atividades dos pesquisadores.

Michel de Certeau (1982) frisava que “cada sociedade se pensa ‘historicamente’ com os instrumentos que lhe são próprios” e que “de resíduos, papéis, legumes, até mesmo de geleiras e de ‘neves eternas’, o historiador faz outra coisa: faz deles história”.

Para Pierre Lévy (1999, p. 92–93), “a codificação digital condiciona o caráter plástico, fluido, calculável com precisão e tratável em tempo real, hipertextual, interativo e, resumindo, virtual da informação que é, parece-me, a marca distintiva do ciberespaço”. Seu entendimento é que essa perspectiva, ou seja, “da digitalização geral das informações tornará o ciberespaço o principal canal de comunicações e suporte de memória da humanidade a partir do início do próximo século”.

Conforme o contexto apresentado, a hipótese desta pesquisa lida com a seguinte proposição: a historiografia baseada em uma investigação científica poderá coletar evidências dos estudos de casos analisados e dos grandes eventos internacionais sediados no país que contribuam para o aprimoramento da defesa cibernética brasileira?

Esta investigação buscou analisar os principais conflitos cibernéticos que de certa forma tiveram um grande impacto mundial, em especial atenção ao Brasil. A pesquisa investigou os ataques cibernéticos mais notáveis, as táticas empregadas e as estratégias de defesa, visando a entender as implicações desses conflitos para a segurança nacional e global. Além disso, descreveu os grandes eventos internacionais realizados no país e o tratamento realizado para a proteção do espaço cibernético em cada um desses eventos, principalmente na forma de atuação para enfrentamento dos possíveis ataques cibernéticos.

A pesquisa foi conduzida utilizando uma abordagem qualitativa, tipificada como descritiva-exploratória no âmbito da tecnologia da informação. Foi realizada uma revisão da literatura, bem como a análise de estudos de casos de incidentes cibernéticos relevantes e os grandes eventos internacionais sediados pelo Brasil entre os anos de 2012 e 2016.

A revisão bibliográfica baseou-se em consultas a diversas fontes de informação necessárias para identificar, avaliar e sintetizar o conjunto de evidências coletadas e elaborado por outros pesquisadores. Foram realizadas consultas, análises e revisões dos seguintes documentos:

- ✓ Conceitos de termos técnicos sobre tecnologia da informação e malwares de computador

- ✓ Conferências sobre crimes cibernéticos
- ✓ Comunidades na Internet sobre segurança cibernética
- ✓ Dicionários convencionais e técnicos
- ✓ Documentos do Wikileaks
- ✓ Literatura relacionada à legislação e normativos referentes à Cibersegurança
    - Leis, Decretos e Portarias
    - Doutrina Militar de Defesa Cibernética
    - Estratégia Nacional de Defesa (END)
    - Estratégia Nacional de Segurança Cibernética
    - Livro Branco de Defesa Nacional
    - Livro Verde Segurança Cibernética no Brasil
    - Política Nacional de Defesa (PND)
    - Política Cibernética de Defesa
    - Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal
- ✓ Rede Nacional de Ensino e Pesquisa (RNP)
- ✓ Relatórios das Forças Armadas Brasileira e do Exército norte-americano
- ✓ Relatórios de Gestão do Tribunal de Contas da União
- ✓ Relatórios estatísticos do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br)
- ✓ Relatórios sobre o legado dos grandes eventos no Brasil – Forças Armadas, CERT.br, FIFA, Comitê Olímpico Internacional, Comitê Olímpico Brasileiro, Comitê Paralímpico Internacional

O trabalho foi organizado em 4 capítulos, sendo o primeiro capítulo a apresentação de um histórico sobre a evolução dos computadores e da Internet no mundo e no Brasil. O conteúdo apresenta um breve relato do uso das mãos e do ábaco para a realização de cálculos matemáticos simples e avança para a lógica matemática no século XVII até o século XX com a ideia de contribuir para liberar o homem das tarefas repetitivas e de simples execução.

Vários nomes importantes da ciência e suas contribuições são destacados, bem como a construção do primeiro computador digital eletrônico totalmente funcional, o ENIAC, e as gerações posteriores até os tempos atuais. O capítulo também trata do

surgimento da informática brasileira, dos primeiros computadores adquiridos pelo país, dos primeiros protótipos de computadores e da fundação da primeira empresa brasileira de fabricação de computadores, a COBRA, durante o regime militar.

Quanto ao surgimento da Internet, são apresentados os principais nomes e as suas contribuições para o desenvolvimento da rede mundial de computadores. A criação da ARPANET no contexto da Guerra Fria e dos movimentos *hippies* norte-americanos, bem como o relato das primeiras tratativas para conectar os centros de pesquisas do Brasil às universidades americanas e a o surgimento da infraestrutura da internet brasileira.

O capítulo 2 aborda quatro estudos de casos sobre conflitos cibernéticos, sendo três estudos de grande impacto internacional e um nacional. O primeiro caso faz um breve histórico da Estônia, localizada no leste europeu, para depois relatar o ataque cibernético sofrido em 2007, que praticamente paralisou os principais serviços governamentais e desconectou o país ciberneticamente do resto do mundo. Sem conectividade a Estônia teve serviços bancários indisponíveis para a população e sofreu com enormes prejuízos financeiros.

O segundo estudo de caso trata da guerra entre a Geórgia e a Rússia em 2008, além de realizar um breve histórico sobre a Geórgia e o fim da URSS. Essa guerra foi considerada a primeira que um ataque cibernético antecedeu um ataque cinético, com objetivo de prejudicar a comunicação do governo georgiano com os seus cidadãos, paralisar os serviços governamentais e obstruir os meios de comunicação do exército da Geórgia no espaço cibernético.

O terceiro caso descreve a contaminação de um vírus de computador, mais conhecido mundialmente como *Stuxnet*, que paralisou o funcionamento de diversas centrífugas de enriquecimento de urânio em Natanz, no Irã, em 2010. Foi o primeiro caso mundial de um vírus utilizado especificamente para sabotar um sistema SCADA de uma infraestrutura crítica[1]. Ou seja, um sistema que geralmente não se conecta à Internet e é usado para comandar máquinas essenciais em instalações de matriz energética, como hidrelétrica, nucleares, petrolíferas, etc.

[1] Infraestruturas críticas são instalações, serviços, bens e sistemas cuja interrupção ou destruição, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade (BRASIL, 2023b).

O único estudo de caso nacional trata dos apagões de energia elétrica no Brasil em 2005, 2007 e 2009 como resultado de um possível ataque cibernético à infraestrutura crítica do país. O assunto foi revelado em um programa jornalístico da rede norte-americana CBS sem que o governo brasileiro fosse consultado sobre o assunto e pudesse se manifestar. Um ano após a reportagem, um vazamento de informações confidenciais do governo norte-americano, conhecido como *Wikileaks*, revelou telegramas secretos enviados pelo Brasil à Embaixada Americana.

O capítulo 3 trata de cinco grandes eventos internacionais sediados pelo Brasil: a RIO +20 (2012), Copa das Confederações (2013), Jornada Mundial da Juventude (2013), Copa do Mundo (2014) e Jogos Olímpicos e Paralímpicos (2016). Eventos que costumam atrair a atenção de milhões de pessoas ao redor do mundo e que por isso se tornam um alvo interessante de ataques cibernéticos. O assunto é abordado com uma breve descrição histórica de cada um desses acontecimentos e o envolvimento do governo brasileiro para controlar as intensas manifestações sociais decorrentes de ciberativismo organizados por grupos centralizadores como *Anonymous e os Black Blocs*.

Por fim, o capítulo 4 trata da revolução digital no 5º domínio conhecido como espaço cibernético e aborda o uso de mercenários digitais para conflagrar ataques cibernéticos em alvos distintos ao redor do mundo. A preocupação da ONU para manter uma certa ordem no espaço cibernético. Apresenta a formação da força cibernética brasileira para fortalecer a defesa e a segurança cibernética e "acende a luz vermelha" quanto ao orçamento e investimento do Brasil em Segurança Cibernética.

O trabalho é histórico e por isso se relaciona com fatos pretéritos, mas serve para lançar o "holofote" quanto à segurança das novas tecnologias que vão surgindo a cada dia. Uma delas é a inteligência artificial, seus benefícios e ameaças. Ainda nessa linha de novidades cibernéticas, há o avanço da robótica, os malefícios das *fake news*, a preocupação com a manipulação voto eletrônico, o uso de moedas digitais, a mudança para prestação de serviços estatais por meio de sistemas digitais totalmente integrados, a crescente necessidade de novos normativos para controle do espaço cibernético, a formação de exércitos cibernéticos, a implementação de controles de segurança, dentre diversas outras novidades que ainda estão a caminho.

Quando se trata de tecnologia, tudo é muito rápido, aparelhos eletrônicos lançados recentemente, em pouco tempo se tornam obsoletos e novas tecnologias vão surgindo

diariamente para substituir as que permanecem por pouco tempo. A história tem essa responsabilidade, de se envolver nos assuntos cibernéticos e coletar dados que sejam relevantes e amparados pela ciência como forma de aprofundar sobre o tema: espaço cibernético.

> O que seria o espaço cibernético? O espaço cibernético é um terreno onde está funcionando a humanidade, hoje. É um novo espaço de interação humana que já tem uma importância enorme sobretudo no plano econômico e científico e, certamente, essa importância vai ampliar-se e vai estender-se a vários outros campos, como por exemplo na Pedagogia, Estética, Arte e Política. O espaço cibernético é a instauração de uma rede de todas as memórias informatizadas e de todos os computadores. Atualmente, temos cada vez mais conservados, sob forma numérica e registrados na memória do computador, textos, imagens e músicas produzidos por computador. Então, a esfera da comunicação e da informação está se transformando numa esfera informatizada. (...) estamos assistindo uma desterritorialização dos textos, das mensagens, enfim, de tudo o que é documento: tanto o texto como mensagem se tornam uma matéria. (...) o espaço cibernético está se tornando um lugar essencial, um futuro próximo de comunicação humana e de pensamento humano. O que isso vai se tornar em termos culturais e políticos permanece completamente em aberto, mas, com certeza, dá para ver que isso vai ter implicações muito importantes no campo da educação, do trabalho, da vida política, das questões dos direitos (LÉVY, 1994).

Mediante o intenso fluxo de informação trafegada na rede mundial e a interdependência tecnológica de todos os serviços prestados em meio digital, tornou-se imprescindível manter esse mecanismo operacional disponível em todo o tempo. Por causa disso, é crescente também o número de ameaças cibernéticas cuja intenção é gerar caos no espaço cibernético.

Preocupados com essa situação, especialistas e governos de todos os continentes têm se empenhado em aumentar a segurança cibernética de suas redes de dados para fins de proteção de seus ativos computacionais. Ela é considerada uma função estratégica de Estado, pois é essencial à manutenção das infraestruturas críticas de uma país, tais como Energia, Defesa, Transporte, Telecomunicações, Finanças, da própria Informação, dentre outras.

Diante de tais desafios, as Nações vêm se preparando, urgentemente, para evitar ou minimizar ataques cibernéticos às redes e sistemas de informação de governo, bem como de todos os demais segmentos da sociedade (BRASIL, 2010).

Para isso são necessárias medidas governamentais que promovam diálogos e intercâmbio de ideias com os diversos segmentos da sociedade para que se apliquem as melhores práticas para a cooperação da cibersegurança no país e entre países. Conscientizar de tais movimentos e as respectivas oportunidades e desafios são

estratégicos para que o Estado Brasileiro se torne uma referência interna e externa sobre esse assunto (BRASIL, 2010).

Nesse sentido, a história desempenha um papel de destaque no contexto da cibersegurança principalmente em relação ao aprendizado com o passado, pois estudar incidentes e ataques cibernéticos pretéritos permite que profissionais de segurança entendam as táticas, técnicas e procedimentos utilizados pelos invasores. Isso possibilita a identificação de padrões e a antecipação de futuros ataques. Contribui para o desenvolvimento de estratégias defensiva, ao analisar casos históricos de violações de segurança; as organizações podem identificar lacunas em suas defesas e desenvolver estratégias mais eficazes para proteger seus sistemas e dados. Reforça a conscientização e a educação sobre a história da cibersegurança e pode ajudar a sensibilizar tanto os profissionais de segurança quanto aos usuários finais sobre os riscos associados às ameaças cibernéticas e a importância da adoção de práticas seguras.

Além disso, ao conhecer a evolução das ameaças cibernéticas ao longo do tempo, os especialistas podem contextualizar as tendências atuais e prever possíveis direções futuras das ameaças, permitindo uma preparação mais eficaz. A história da cibersegurança investiga como a computação e a Internet evoluíram ao longo do tempo, desde seus estágios iniciais até as complexidades atuais. Isso ajuda a demonstrar a maturidade tecnológica e a destacar a importância contínua da inovação e da adaptação frente às ameaças cibernéticas.

Em resumo, a história tem um papel estratégico em retratar a evolução da cibersegurança, fornecendo lições valiosas, fatos históricos e uma base de conhecimento para a melhoria contínua da segurança cibernética brasileira e mundial.

1. Um histórico sobre a evolução dos computadores e da Internet no mundo e no Brasil

Para Georges Ifrah (1997, p. 91–92) a mão pode ser reconhecida como a forma mais antiga e a mais difundida no auxílio para a realização de contas e de cálculo, empregado pelos povos no curso da história. O procedimento consiste em atribuir um valor inteiro a cada dedo, na ordem de sucessão regular começando pela unidade, por isso

é apontada como a primeira máquina de contar da humanidade. Tertuliano declamava no seu Discurso apologético que era preciso permanecer de pé envolto por uma grande quantidade de papéis e gesticulando os dedos para exprimir os números.

Segundo Fernandes (2006, p. 15–16), as pedras foram consideradas os primeiros objetos utilizados que iniciaram as pessoas na arte de calcular e estão presentes na formação da origem dos ábacos, compreendidos como contadores mecânicos. A técnica viabilizou um sistema de contagem silenciosa, sem a necessidade de memorização e de conhecimentos complexos de números. "A palavra ábaco é romana e deriva do grego *abax* ou *abakon*, significa superfície plana ou tábua" e pode ser conhecido com nomes diferentes em outros países como: "China – *Suan Pan*; Japão – *Soroban*; Coréia – *Ts-chu Pan*; Vietnam – *Ban Tuan* ou *Ban Tien*; Rússia – *Schoty*; Turquia – *Coulba*; Armênia – *Choreb"*. No caso do ábaco romano, criado antes da era cristã, era utilizado como se fosse uma calculadora de bolso para que cálculos aritméticos fossem realizados de forma simples e rápida (SILVA, 2011, p.16).

1.1. A evolução dos computadores

Mas o que seria das ciências da computação sem a lógica matemática moderna, que começou no século XVII com os estudos de Gottfried Wilhelm Leibniz. De acordo com Cléuzio Filho (2007, p. 49) "seus estudos influenciaram, 200 anos mais tarde, vários ramos da Lógica Matemática Moderna e outras áreas relacionadas, como por exemplo a Cibernética". Para Leibniz, a Metafísica precisava de um instrumento suficientemente poderoso que alcançasse o mesmo grau de rigor da Matemática. Conforme demonstrado pela história, diversos pensadores contribuíram para um novo simbolismo matemático:

> Descartes e Fermat criaram a geometria analítica, e, depois de iniciado por Galileu, o cálculo infinitesimal desenvolveu-se com grande rapidez, graças a Newton e ao próprio Leibniz. Ou seja, as matemáticas romperam uma tradição multissecular que as havia encerrado no âmbito da geometria, e estava se construindo um simbolismo cada vez mais fácil de manejar e seguro, capaz de funcionar de uma maneira, por assim dizer, mecânica e automática, sujeito a operações que, no fundo, não eram mais do que regras para manipulação de símbolos, sem necessidade de fazer uma contínua referência a conteúdos geométricos intuitivos (FONSECA FILHO, 2007, p. 50).

A Leibniz atribuiu-se também o desenvolvimento de base de numeração binária. A numeração binária utiliza somente dois coeficientes: 0 e 1, bastam os dois dígitos para elaborar as tabuadas da soma e da multiplicação (SANTOS; PEDRO NETO; SILVA, 2007, p. 11). E conforme suas anotações particulares havia uma preocupação em fazer do

conhecimento algo de útil, mesmo que os frutos fossem colhidos por outros e não pelo autor, e quanto ao mal incurável se referia a questão da ignorância fosse tomada pela aversão ao estudo.

> Tenho pensado comigo muitas vezes que os homens poderiam ser muito mais felizes do que são, se aquilo que eles potencialmente têm, também o pudessem ter efetivamente, para que, assim que precisassem, pudessem usá-lo. Ora, a verdade é que nós mesmos não conhecemos nossas potencialidades; somos como um negociante que não faz o livro-caixa ou como uma biblioteca sem fichário. E também, do modo como agimos, talvez possamos ser úteis a nossos longínquos descendentes, nós próprios não colheremos os frutos de nossos trabalhos; vamos discutindo, vamos acumulando sem parar e raramente acabamos demonstrando algo ou fazemos disso um inventário; mal tiramos proveito de nossos estudos. E se assim continuarmos, deveremos cuidar para não ser atingidos por um mal incurável <e para que a ignorância não seja restaurada pela aversão ao estudo>, quando a exagerada quantidade de coisas e livros suprimir qualquer esperança de discernimento e o que é estável e útil for obscurecido pela massa de coisas sem valor (USP, 2007).

Para Fonseca Filho (2007, p. 86–87), a ideia de Leibniz contribuiu para liberar o homem das tarefas repetitivas e de simples execução, e foi quase colocado em prática por Charles Babbage, após apresentar um projeto de mecanismo feito de madeira e latão em 1822, capaz de executar uma série de cálculos. Conhecida como máquina diferencial, era capaz de resolver equações polinomiais, o que permitiu a construção de tabelas de logaritmos, um dos maiores problemas na época (SARAIVA, 2009).

Em 1823, Babbage realizou um financiamento do governo britânico que possibilitou a construção de um dispositivo capaz de resolver qualquer tipo de cálculo. Essa sua invenção viria ser conhecido um dia como computador, batizada de Máquina Analítica (SARAIVA, 2009). Jack Copeland (2006) destacou que Babbage trabalhou em parceira com Ada Lovelace, criadora dos primeiros fundamentos de programação, tendo desenvolvida vários programas. Atualmente seu nome é associado à moderna linguagem de programação ADA.

Já o matemático George Boole desenvolveu, em 1947, um sistema lógico utilizando os algarismos: 0 ou 1. De acordo com a sua teoria, o número “1” significava ativo, ligado, existente e verdadeiro. O número “0” representava o inverso, ou seja, o não ativo, desligado, não existente, falso. Atualmente, todo sistema lógico dos computadores faze uso da teoria de Boole de forma prática (GUGIK, 2009, p.03), com a introdução da unidade de informação conhecido como *Bit* (*Binary digit*).

Herman Hollerith introduziu o conceito de cartões perfurados, utilizados na máquina mecanográficas ou tabuladoras, que acelerou o processamento dos dados do censo dos Estados Unidos no ano de 1890. Para fins de entendimento, o censo anterior

levou 7 anos e meio para ser processado e concluído, com o uso da máquina de Hollerith o censo foi processado em 3 anos e meio. O nome de Hollerith está associado ao uso do cartão perfurado, que foi utilizado até o final da década de 80 (CARDI, 2002, p. 18).

Em 1935, a revolução do computador começou efetivamente a realizar-se com a participação de Alan Mathison Turing, na época estudante do King´s College em Cambridge. Turing desenvolveu diversos trabalhos importantes que resultaram na fundamentação teórica da chamada "Ciência da Computação". Ele formalizou definitivamente o conceito de algoritmo (FONSECA FILHO, 2007, p. 74–75). "Turing também desenvolveu um teste para comprovar se um computador possuía ou não inteligência artificial" (SARAIVA, 2009). Além disso, durante a II Guerra Mundial, Turing foi convocado pela Escola de Cifras e Códigos, cuja tarefa era decifrar mensagens codificadas do inimigo, mais conhecida como a "Máquina Enigma". "Quando a guerra terminou, Turing tinha ajudado a construir um computador, o Colossus, uma máquina inteiramente eletrônica com 1.500 válvulas (...)"(FONSECA FILHO, 2007, p. 78).

O Colossus Mark 1 foi considerado o primeiro computador digital programável, cuja utilização ocorreu principalmente em consequência da II Guerra Mundial. O computador Colossus Mark 2 tornou-se o primeiro a ser produzido em série, com 10 unidades no total. No entanto, esse computador fazia parte de um projeto secreto do governo inglês, que fez que seus inventores não recebessem crédito e o design também não pôde ser aproveitado em outros computadores. O projeto do Colossus acabou na obscuridade (MORIMOTO, 2011).

Mas os norte-americanos foram mais liberais quanto ao compartilhamento de informações e construíram o ENIAC (*Electronic Numerical Integrator Analyzer and Computer*) entre os anos de 1943 e 1945. No entanto, sua operação ocorreu somente em 1946, encerrando suas operações em 1955. O ENIAC foi o primeiro computador digital eletrônico totalmente funcional a ser construído pela Escola Moore de Engenharia Elétrica da Universidade da Pensilvânia - Estados Unidos, para atender um pedido do Departamento do Exército Americano. O computador foi idealizado por Presper Eckert e John Mauchly, ele era um pouco semelhante ao Colosso, embora fosse maior e mais flexível. Foi projetado para realizar cálculos das tabelas usadas pela artilharia (COPELAND, 2006). Outros computadores foram construídos, como o UNIVAC I (*Universal Automatic Calculator*), em 1951, o primeiro computador comercialmente disponível.

Desde então, houve uma revolução do hardware e do software, diversas linguagens de programação foram desenvolvidas e as arquiteturas de máquinas, principalmente impulsionadas pela invenção do transistor (1948). Outros equipamentos eletrônicos passaram a ter espaço no ambiente computacional, tais como impressoras, as fitas magnéticas, os discos para armazenamento, etc. Segundo Cléuzio Filho (p.123), “os computadores passaram a ter um desenvolvimento rápido, impulsionados principalmente por dois fatores essenciais: os sistemas operacionais e as linguagens de programação”.

Todas as transformações do computador foram se aperfeiçoando ao longo do tempo, isso se deve ao avanço das áreas da matemática, eletrônica, engenharia da computação. Anshuman Singh (2023) descreveu a história da computação em cinco gerações:

- Primeira Geração (1946 – 1959) – esses computadores usavam tecnologia de válvula eletrônica que tornavam os computadores caros e acessíveis apenas a grandes corporações. A linguagem de programação era linguagem de máquina e não podia realizar multitarefas, além de serem imensos, pesados e consumirem muita energia.
- Segunda Geração (1959 – 1963) – esses computadores substituíram as válvulas eletrônicas por transistores, tornando-se menores, mais rápidos e mais eficientes. Os transistores eram mais eficientes que os tubos de vácuo, exigiam menos manutenção e geravam menos calor. Esses computadores eram menores e mais portáteis, tornando-os acessíveis a um público mais amplo. A memória de núcleo magnético também foi introduzida nesta geração.
- Terceira Geração (1964 – 1971) – esses computadores utilizavam microchips ou circuitos integrados, possibilitando a criação de computadores menores, mais baratos e muito mais rápidos. Foram introduzidos novos dispositivos de entrada, como mouse e teclado, substituindo métodos antigos, como cartões perfurados. Novas funcionalidades foram utilizadas como multiprogramação e processamento remoto.
- Quarta Geração (1972 aos dias atuais) – esses computadores utilizavam microprocessadores em larga escala e eram capazes de realizar atividades e cálculos complexos. Utilizavam maior capacidade de processamento e

armazenamento, sendo mais rápidos e eficientes que os computadores das gerações anteriores. Eles se tornaram portáteis, pequenos e consumiam menos energia. Essa geração teve os primeiros supercomputadores que utilizavam linguagens de programação complexas como C, C++, DBASE, etc.

- Quinta Geração (em desenvolvimento): esses computadores utilizarão inteligência artificial (IA) para a realização de tarefas super complexas, como reconhecimento de imagens, interpretação da fala humana, compreensão de linguagem natural.

Quanto ao surgimento da informática brasileira, o Museu do Computador da Universidade Estadual de Maringá (UEM, 1996), descreve que o seu desenvolvimento ocorreu em duas etapas. A primeira, de 1958 até 1975 e a segunda a partir de 1976. No Apêndice A é apresentado um quadro com alguns dos principais eventos cronológicos da Informática Brasileira.

A primeira etapa foi caracterizada pela importação de tecnologia de países desenvolvidos, principalmente dos Estados Unidos. Os computadores de grande porte adquiridos eram utilizados por grandes empresas brasileiras, universidades e por alguns órgãos governamentais e agências de serviços (UEM, 1996).

Até o final da década 1950, os computadores eram raridade curiosa e quase inacessível no Brasil. Seus usuários eram poucos e podiam ser contabilizados.

> O primeiríssimo foi adquirido pelo governo do Estado de São Paulo, em 1957: um Univac 120 para calcular o consumo de água na capital. Equipado com 4.500 válvulas, fazia 12 mil somas ou subtrações por minuto e 2.400 multiplicações ou divisões, no mesmo tempo. No setor privado, o primeiro computador, um Ramac 305 da IBM, foi comprado em 1959, pela Anderson Clayton. Dois metros de largura, um metro e oitenta de altura, com mil válvulas em cada porta de entrada e saída da informação, ocupava um andar inteiro da empresa. A unidade de disco, com 150 mil bytes de capacidade e um único braço de acesso, tinha dois metros de altura, exibindo-se em uma redoma de vidro. Levava cinco minutos para procurar uma informação. A impressora operava à espantosa velocidade de 12,5 caracteres por segundo (DANTAS, 1988).

O impulso para o avanço da informática no Brasil ocorreu no governo de Juscelino Kubitschek. Em 1958, foi autorizada a criação de um grupo de trabalho cuja finalidade era estudar a viabilidade da utilização de máquinas de cálculo na administração e no apoio ao uso de recursos financeiros de seu Plano de Metas, com o objetivo de fazer o país "crescer 50 anos em cinco", uma visão baseada no desenvolvimento econômico planejado e destinado a tirar o país do atraso (DANTAS, 1988).

> A criação do grupo de trabalho lhe foi sugerida pelo secretário-geral do Conselho de Desenvolvimento Nacional, o economista Roberto de Oliveira Campos que aceitou as ideias do capitão-de-corveta Geraldo Maia, recém-chegado de uma pós-graduação em engenharia eletrônica nos Estados Unidos, e convencido da importância e absoluta necessidade de o país utilizar computadores no momento em que pretendia dar um pulo em seu desenvolvimento (DANTAS, 1988).

O grupo apresentou em janeiro de 1959 um relatório com uma série de sugestões para incentivar a implantação de centros de processamentos de dados no país, sendo uma delas, o CPD do governo federal. Em razão disso, surge no dia 13 de outubro de 1959 o Grupo Executivo para Aplicação de Computadores Eletrônicos (GEACE), com a finalidade de aprovar concessão de benefícios à aquisição de computadores, principalmente isenções de impostos de importação e sobre produtos industrializados (DANTAS, 1988). Enquanto funcionou, a GEACE aprovou as importações dos seguintes computadores:

- B205, da Burroughs para a Pontifícia Universidade Católica do Rio de Janeiro – PUC-RJ;

> Como naquela época, não havia avião comercial com espaço suficiente para transportar o equipamento, de grande porte ao Brasil, o país recebeu o auxílio da extinta empresa Pan American, que disponibilizou um DC7C para o transporte do B-205 de Los Angeles (Estados Unidos) até o antigo Aeroporto do Galeão, no Rio de Janeiro (Brasil). O equipamento chegou ao solo brasileiro no final do ano de 1959. O B-205 era um computador completamente diferente dos que conhecemos hoje, pois ocupava uma sala inteira. O chamado “cérebro eletrônico” era um Burroughs Datatron 205, da primeira geração de computadores a válvulas (ele possuía cerca de 4.600), efetuava uma adição em 0,1 milissegundos e a memória era uma espécie de tambor magnético com capacidade a cerca de 20K bytes. A entrada de dados era feita através de cartões e fitas perfuradas, além de teclado manual. Os dados eram armazenados em fitas magnéticas, parecidas com as fitas utilizadas em cassetes, só que em rolos. A programação era efetuada em linguagem de máquina absoluta, não possuía sistema operacional, sistema de arquivos, processador de linguagem ou qualquer outro software de apoio. Trabalhava apenas em ponto fixo e em consequência tinha uma lâmpada "Overflow" que significava ter de começar fazendo nova escolha de escalas para as variáveis (coisas que desapareceram com os progressos dos programas). A “impressora” era um tipo de máquina de escrever *flexowriter* com velocidade de dez caracteres por segundo. Posteriormente foi agregada uma tabuladora IBM 407, que expandiu a velocidade de impressão para cem linhas por minuto. Finalmente, em 1960, foi inaugurado o primeiro computador da América Latina em Universidades e o primeiro do Brasil, no recém-criado Centro de Processamento de Dados da PUC-RJ. Na época da inauguração a PUC do Rio recebeu a visita do Cardeal Montini de Roma, que mais tarde tornou-se o Papa Paulo VI. Pelo seu alto posto ele foi convidado para inaugurar o computador, como também o Presidente da República Juscelino Kubistchek. Assim, o então Cardeal Montini inaugurou o Primeiro Centro de Processamento de Dados do país e o presidente Juscelino inaugurou o computador. O equipamento teve o mérito de mostrar aos estudantes, entre outras coisas, novas técnicas de cálculos científicos para aplicação em várias áreas de engenharia e pesquisa (CARDI; BARRETO, 2012).

- Univac 1103 para o Instituto Brasileiro de Geografia e Estatística – IBGE;
- Gama, da Bull, para a empresa Listas Telefônicas Brasileiras.

Além disso, o GEACE promoveu em abril de 1960 o primeiro Simpósio sobre Computadores eletrônicos, no auditório do Ministério da Educação, na cidade do Rio de Janeiro. A sua extinção ocorreu no governo de Jânio Quadros à Presidência da República, pois considerou cumpridas as suas finalidades (DANTAS, 1988).

O desenvolvimento e a construção dos primeiros protótipos de computadores surgiram nas universidades nacionais como projeto de conclusão dos cursos de graduação em engenharia (CARDI; BARRETO, 2012):

- Lourinha (nome informal) - do Instituto Militar de Engenharia (IME): iniciou-se o projeto de computadores, efetivado a partir de 1958 (parte analógica), combinando com o projeto de fim de curso da turma de 1960. Criaram um computador que além da parte digital incluía circuitos analógicos capazes de simular, em tempo real, sistema de equações diferenciais e com isto resolver problemas complexos. Hoje esta parte de circuitos analógicos seria implementada por programas de simulação tais como ACSL (*Analog Computer Simulation Language*) ou o clássico CSMP (*Continuous System Modeling Program*).

  > Após a defesa do projeto a máquina foi desmontada e transformada em placas para o estudo da Arquitetura de Computador, peça usada até os anos 70 no Laboratório de Circuitos Digitais. Portanto, Lourinha cumpriu sua finalidade e a História da Computação no Brasil ganhou um novo marco. Na época do episódio o trabalho não foi divulgado por recomendação da direção da Escola Técnica do Exército. Com efeito, pouco antes a Rússia havia enviado o primeiro satélite artificial e pouco depois um satélite tripulado por uma cadela de nome Kudriavka que ficou conhecida como Laika. Conta-se que um repórter, sabendo que na Escola Técnica do Exército estava em andamento um projeto de confecção de foguetes, foi à Escola e, procurando um "furo de reportagem" perguntou se seria enviado algum animal em órbita e, a negativa sob a forma de risos, foi interpretada como uma afirmativa provocando reação dos protetores de animais e a consequente recomendação de sigilo da direção sobre os projetos em andamento. O computador teve um destino trágico, em uma limpeza do Departamento de Engenharia do IME, por problema de espaço, ele foi desmontado e consequentemente o seu fim foi o "lixo" (CARDI; BARRETO, 2012)

- Zezinho[2] (denominada ITA I - 1961) - do Instituto Tecnológico da Aeronáutica (ITA): foi construído com transistores discretos, usando soquetes de válvulas para demonstração e uso em laboratório. Tinha dois metros de largura por um metro e meio de altura.

[2] Embora um sucesso, o Zezinho não sobreviveu durante muito tempo. Foi desmontado aos poucos pelos alunos das turmas seguintes, que utilizaram seus circuitos para novas experiências. Tampouco foi considerado um trabalho superior ao de outros alunos da mesma turma, como um sistema de FM estéreo que gerou uma patente, ou um sistema de circuito fechado de televisão (DANTAS, 1988).

- Patinho Feio (julho de 1972) - do Laboratório de Sistemas Digitais (LSD) do Departamento de Engenharia da Eletricidade da Escola Politécnica da Universidade de São Paulo - composto de 450 pastilhas de circuitos integrados, contendo cerca de três mil blocos lógicos, distribuídos em 45 placas de circuito impresso e cinco mil pinos interligados segundo a técnica '*wire-wrap"*. A memória principal tinha capacidade para 4.096 palavras de oito bits. A nomenclatura "Patinho Feio" surgiu de uma brincadeira com um projeto da Marinha chamado Cisne Branco, muito comentado pela mídia nacional. Assim, o nome revelava, por si só, a autoestima da produção tecnológica.
- G -10[3] - protótipo de computador do Laboratório de Sistemas Digitais da USP (que faria o "hardware") e do Departamento de Informática da PUC do Rio de Janeiro (que faria o "software"), que foi entregue em 1975. Tinha as características de um protótipo, o que não aconteceu com o Patinho Feio. Possuía documentação com desenhos e especificações, software e sistema operacional desenvolvido pela PUC-RJ.

No governo Médici, um das metas do Plano Nacional de Desenvolvimento (PND) era o de promover o desenvolvimento tecnológico e nesse sentido foi criado o Grupo de Trabalho Especial (GTE) por meio do Decreto nº 68.267 de 18 de fevereiro de 1971, o que possibilitou um acordo entre a Marinha brasileira, o Ministério do Planejamento e o BNDE para projetar e fabricar um computador de tecnologia nacional para fins de operações navais (HELENA, 1984, p.12).

O interesse do segmento militar e científico para que o país atingisse sua independência tecnológica, levou à criação da CAPRE (Comissão de Coordenação das Atividades de Processamento Eletrônico), no dia 5 de abril de em 1972 por meio do Decreto nº 70.370, com a finalidade de adotar e propor medidas visando à racionalização

[3] Em setembro de 1977, no VII Secomu, realizado em Florianópolis/SC, sob influências da Capre e da Finep que estava financiando o projeto, os executivos da empresa Cobra comprometeram-se a tocar o projeto do G-10 de forma mais efetiva. A máquina foi reprojetada, passando a ser designada de G-11. Multiusuário, mas ainda sem o efetivo comprometimento da Cobra na sua industrialização. Porém, quando houve a decisão da Cobra em assegurar o projeto, a máquina foi novamente reprojetada, originando a linha Cobra 500 (CARDI; BARRETO, 2012).

dos investimentos governamentais no setor e à elevação da produtividade na utilização dos equipamentos de processamento de dados instalados e a instalar (BRASIL, 1972).

Em 18 de julho de 1974, por meio da parceria com o Banco Nacional de Desenvolvimento Econômico (BNDE) era fundada a primeira empresa brasileira de fabricação de computadores, a COBRA[4] (Computadores e Sistemas Brasileiros Ltda) (HELENA, 1984, p.09), uma estatal que recebeu a missão de transformar o G-10 em um produto nacional (UEM, 1996). Tratava-se da formação de uma sociedade em que os majoritários possuíam cada um cerca de um terço da companhia. A saber a E.E (Equipamentos Eletrônicos), a Ferrantil, companhia inglesa fabricante de computadores e a DIGIBRÁS (Empresa Digital Brasileira S.A), estatal de fomento à indústria eletrônica (HELENA, 1984, p.9).

A virada para a segunda etapa do desenvolvimento da informática no Brasil iniciou-se em 1976 e caracterizou-se pelo surgimento de uma indústria nacional, pois até então o que se tinha eram as primeiras empresas montadoras multinacionais. Nesse sentido, foi realizada a restruturação da CAPRE e a criação de uma reserva de mercado na faixa de minicomputadores para empresas nacionais e pelo controle das importações (UEM, 1996).

Ainda em 1976 a competência da CAPRE foi ampliada e tornou-se uma comissão de assessoria à Presidência da República na formulação de um modelo de política industrial de informática (MARCELINO, 1983, p.90). Em 15 de julho, a CAPRE estabeleceu uma resolução (01/76) com o objetivo de criar reserva de mercado de minissistemas e periféricos para a iniciativa nacional (SANTOS, 2003, p.24).

A disputa sobre a criação de uma reserva de mercado do Brasil para a faixa de computadores de pequeno porte com recursos predominantemente nacionais se intensificou a partir da segunda metade dessa década. Diante do debate gerado, “a CAPRE foi acusada de ser internacionalista e consequentemente extinta, criou-se então em 1979 a Secretaria Especial de Informática (SEI), em substituição àquela Coordenação

[4] O nome "Cobra" surgiu por acaso, conta ainda Uchoa, numa reunião havida, às vésperas da fundação da empresa, O nome tinha que sair dali. Havia pressa para o registro de papéis e providências burocráticas. Uchoa gostaria de incluir no nome a palavra "Guaranys’’, que, além de ser um nome bem brasileiro, constituiria uma homenagem a seu companheiro de Marinha, o comandante Guaranys, personagem de destaque nas idas e vindas que culminaram com a criação de uma empresa brasileira de computadores. Mas foi um inglês, Mr. Herbert Bray - que viria a ser o primeiro diretor técnico da Cobra - o autor da sugestão vencedora. Uma sigla que escreveu partindo da ideia "computadores brasileiros’’, com a união das duas sílabas iniciais destas palavras (HELENA, 1984).

(MORAES, 2016, p.27). O Decreto nº 84.067/79 de criação da SEI e assinado pelo presidente Figueiredo, a estabeleceu como órgão complementar do Conselho de Segurança Nacional (CSN) e extinguiu a CAPRE (DANTAS, 1988). Caberia à SEI assessorar na formulação da Política Nacional de Informática (PNI) e coordenar a sua execução de forma direta ou indiretamente, tendo em vista, especialmente, o desenvolvimento científico e tecnológico do setor, bem como promover e incentivar a utilização da Informática como meio de agilização do processo decisório e do desenvolvimento nacional (BRASIL, 1979).

> Em 1978 a IBM encaminha à CAPRE proposta de fabricação de computadores de médio porte para fazer frente ao crescente mercado de minicomputadores nacionais desestabilizando assim o mercado. Em novembro, dois modelos maiores do pacote de cinco máquinas apresentados pela IBM são aprovados, sem unanimidade, pela CAPRE. Nesse quadro, respaldado pelo governo, entra em cena o SNI (Serviço Nacional de Informações), o CSN (Conselho de Segurança Nacional) e o MRE (Ministério das Relações Exteriores), que passam a atuar de maneira sigilosa no estudo da viabilidade de formação de uma indústria nacional de componentes e produtos finais pelas próprias empresas brasileiras (SANTOS, 2003, p.24).

Somente em outubro de 1984 a Política Nacional de Informática foi sancionada pelo Congresso (Lei nº 7232/84), com a finalidade de manter os mercados de mini e microcomputadores para as empresas nacionais. O interesse do governo brasileiro era de manter uma política industrial protecionista, por meio da reserva de mercado, a fim de favorecer a produção nacional em setores econômicos e ser menos dependente das grandes companhias estrangeiras que já dominavam os mercados (FIGUEIREDO, 1986, p.287). Com isso o Poder Executivo poderia estabelecer limites à comercialização, no mercado interno, de bens e serviços de informática, mesmo produzidos no país, sempre que ela implicasse na criação de monopólio de fato em segmentos do setor, conforme o art. 10 da referida lei (BRASIL, 1984).

A participação de empresas não-nacionais no mercado brasileiro limitou-se a produção de itens de informática que não existissem nas empresas nacionais capacitadas para produzi-los, mesmo assim condicionadas a apresentação de planos de exportações e pesquisa e desenvolvimento (P&D) no país. Desta forma, o caráter regulador e interventor do Estado tornou-se juridicamente instituído e permitido enquanto as empresas nacionais não apresentassem capacitação para competir no mercado mundial (TONOOKA, 1992, p.284-285).

O setor empresarial do País além da reserva de mercado também usufruiu de uma série de incentivos para a realização de projetos de pesquisa, desenvolvimento e produção de bens e serviços de informática, tais como:

a) isenção e redução nos impostos de importação e exportação, IPI, imposto sobre operações de crédito e IR;
b) permissão para depreciação acelerada;
c) prioridade para obtenção de financiamentos públicos;
d) redução do lucro tributável para os setores de microeletrônica e software;
e) Criou-se também um mecanismo para pessoas jurídicas investirem na compra de ações de empresas nacionais de informática, via dedução no imposto de renda devido (TONOOKA, 1992, p. 284–285).

Todo esse protecionismo da indústria de informática nacional passou por uma nova concepção partir do início da década de 90, com uma série de modificações introduzidas na PNI, com intuito de adequá-la a uma nova fase nas relações entre o Estado e o setor de informática. Principalmente com uma maior abertura ao mercado externo, postas em prática pelo governo do presidente Fernando Collor, ditas como políticas econômicas liberais, com a premissa da necessidade de maior abertura, ao comércio exterior e ao capital estrangeiro, com isso ocorreu:

f) a reestruturação dos órgãos responsáveis pela PNI, extinguindo a SEI, em 12 de abril de 1990, através da Lei n° 8.028/90;
g) a substituição da SEI, pelo Departamento de Política de Informática e Automação (DEPIN), vinculado à Secretaria de Ciência e Tecnologia da Presidência da República (SCT), em 11 de setembro de 1990, através da MP n° 222.
h) a eliminação da anuência prévia sobre a importação de determinados produtos de informática, em 21 de setembro de 1990, através do Decreto n° 99.541 e Resolução n° 20 da SCT; e
i) o relaxamento da aplicação da reserva de mercado, autorizando a formação de *joint-ventures*; em 11 de outubro de 1990, através da Resolução n° 19, da SCT (MOREIRA, 1995, p.37).

Em 29 de outubro de 1992, por decurso de prazo, a Política Nacional de Informática expirou, mesmo porque a PNI já estava sendo burlada tanto pela iniciativa

privada quanto pelo governo. Este, sancionado por leis que buscavam alternativas que minimizassem os impactos da reserva de mercado, por outro lado, a indústria de informática buscava obter, via contrabando, componentes básicos (microprocessadores, chips, memória, etc) para montagem de máquinas, encomendadas pelo próprio governo e/ou empresas estatais. Dificilmente o que se pretendia com isso era descobrir a tecnologia desenvolvida para reprodução de máquinas semelhantes ou mesmo a construção de modelos mais avançados (MOREIRA, 1995, p.37).

1.2. Surgimento da Internet

Pode-se dizer que não existe um único criador da Internet, na verdade muitos foram os pais da Internet, pois ela não foi obra e nem inspiração de apenas uma pessoa. Ela começou a ganhar vida em 1958 e desenvolveu-se num ambiente acadêmico com financiamento da *Advanced Research Projects Agency* (ARPA), uma agência militar de pesquisas ligada ao Departamento de Defesa (DoD) norte-americano. O nome original ARPA foi alterado em março de 1972 e passou a se chamar DARPA (*Defense Advanced Research Projects Agency*) com a adição da palavra "defesa" na sigla (OLIVEIRA, 2011, p.23).

A gênese dessa missão e da própria DARPA remonta ao lançamento do primeiro satélite artificial, o Sputnik I[5] em outubro de 1957. Um evento que chocou os Estados Unidos. Na época, muitos norte-americanos temiam que o país estivesse perdendo liderança tecnológica ao seu adversário da Guerra Fria. Após o lançamento do primeiro Sputnik, o presidente Dwight D. Eisenhower seguiu o conselho do secretário de Defesa Neil McElroy e principais cientistas e propôs a criação da ARPA (ATTA, 2018, p. 12).

Inicialmente a agência concentrou-se em três atribuições do presidente: espaço, mísseis de defesa e detecção de testes de armas nucleares. No entanto, Eisenhower enfatizou que o espaço seria o domínio de uma agência civil. Para esse fim, mais tarde em 1958, o Congresso e o presidente criaram a *National Aeronautics and Space*

[5] A liderança soviética durou vários anos, com o lançamento do primeiro ser vivo ao espaço (a cadela Kudriavka, da raça Laika), da primeira nave a pousar na Lua (Lunik 2), da primeira nave a fotografar o outro lado da Lua (Lunik 3), do primeiro astronauta (Yuri Gagarin), do primeiro voo conjunto de duas espaçonaves (Vostok III e IV), da primeira mulher ao espaço (Valentina Tereshkova), da primeira nave a levar mais de um tripulante (Voskhod 1), do primeiro astronauta a "caminhar" no espaço (Alexei Leonov), além da espaçonave com maior período de uso na história da exploração espacial (Soyuz) (CARVALHO, 2006, p.08).

Administration (NASA), uma entidade civil responsável pelos principais programas espaciais do país. Como tal, a NASA absorveu grande parte do programa espacial da DARPA (ATTA, 2018, p. 12).

Logo após a sua fundação, a DARPA assumiu o Projeto AGILE, um programa altamente confidencial de uma década que apoiava os esforços dos EUA no Vietnã, proposta pelo seu vice-diretor, William Godel. O projeto AGILE foi administrado com pouca supervisão; não era nada científico e focado em soluções de curto prazo. O projeto serviu de lição do que a DARPA não deveria fazer (ATTA, 2018, p. 13).

> Com a transferência do programa espacial para a NASA, a DARPA passou a década de 1960 concentrada na defesa antimísseis, detecção de testes nucleares e AGILE. No início da década de 1960, contudo, a DARPA começou a seguir um conjunto de empresas menores, programas tecnicamente focados para prevenir surpresas tecnológicas. Os programas iniciais se basearam em ciência dos materiais, tecnologia da informação, e ciência comportamental. Indiscutivelmente, a DARPA inventou estas áreas para realizar buscas tecnológicas. Por exemplo, em 1961, o diretor da DARPA, Jack Ruina contratou Joseph C.R. Licklider como o primeiro diretor do Escritório de Técnicas de Processamento de Informação (em inglês: Information Processing Techniques Office - IPTO), que desempenhou um papel vital na criação da computação pessoal e da ARPANET, a base para a futura Internet (ATTA, 2018, p.13).

Joseph Licklider tinha como experiência o fato de ter sido pesquisador do Instituto de Tecnologia de Massachussets (MIT) sobre a interação entre computadores e usuários, além de ter estudado física, matemática e psicologia. Ainda no início da década de 60, publicou uma série de artigos referente à possibilidade de utilizar computadores interconectados para compor uma comunicação global com acesso a bibliotecas eletrônicas. Os memorandos de Licklider ficaram famosos os quais chamavam os seus colegas de "membros da comunidade intergaláctica de computadores" (OLIVEIRA, 2011, p.23).

Licklider trouxe para a DARPA a visão de um conceito revolucionário de computadores e como eles poderiam ser usados. Ele previu que, em vez de ser fundamentalmente máquinas de calcular, os computadores poderiam ser empregados como ferramentas de apoio aos seres humanos em processos criativos, discutido no artigo "Simbiose Homem-Computador" de março de 1960 (ATTA, 2008, p.40). O objetivo fundamental era explorar a complementação entre as capacidades humanas e as capacidades dos computadores que deveriam apresentar:

a. Seleção de metas e os critérios – capacidade humana;
b. Formulação de questões e hipóteses – capacidade humana;
c. Seleção de abordagens – capacidade humana;

d. Deleção de relevância – capacidade humana;
e. Reconhecimento de padrões e objetos – capacidade humana;
f. Tratamento de imprevistos e baixa probabilidade de exigência – capacidade humana;
g. Armazenamento de grande quantidade de informações, com grande precisão – capacidade computacional;
h. Recuperação de informações rapidamente – capacidade humana e computacional; com grande precisão – capacidade computacional;
i. Cálculos rápidos e assertivos – capacidade computacional;
j. Montagem de forma progressiva de um repertório de procedimentos sem sofrer perdas devido a uma interferência ou falta de uso – capacidade computacional (LICKLIDER; CLARK, 1962, p.114).

No entanto, para fazê-lo exigir-se-iam capacidades informáticas inteiramente novas, ainda inexistentes que incluía computadores interativos, computação pela Internet, realidade e sistemas inteligentes. A extraordinária noção de Licklider de "simbiose homem-computador" previa o uso de novos tipos de capacidades computacionais para alcançar capacidades humanas aumentadas e até mesmo a inteligência artificial. Essa noção tornou-se o nascimento de um esforço concentrado que resultou na ARPANET, além de propiciar a evolução tecnológica, como inovação em computação gráfica, melhoria no processamento dos computadores e outros desenvolvimentos, que possibilitariam a concretização da visão de se conectar computadores pessoais (ATTA, 2008, p.40).

> O compromisso dos Estados Unidos de que, a partir de então, seria o iniciador e não a vítima de surpresas tecnológicas estratégicas. Trabalhando com inovadores dentro e fora do governo, a DARPA cumpriu repetidamente essa missão, transformando conceitos revolucionários e até mesmo impossibilidades aparentes em capacidades práticas. Os resultados finais incluíram não apenas capacidades militares revolucionárias, como armas de precisão e tecnologia furtiva, mas também ícones da sociedade civil moderna, como a Internet, reconhecimento de voz automatizado e tradução de idiomas, e receptores de Sistema de Posicionamento Global pequenos o suficiente para serem incorporados em uma infinidade de dispositivos de consumo (DARPA, 2024)

No início, após algumas tentativas sem sucesso feitas pela DARPA, para conectar computadores, com a chegada Leonard Kleinrock[6], a situação alterou-se. Quando ainda

[6] Na época, imaginei que a rede seria sobre pessoas conversando com computadores, computadores conversando com computadores, mas não sobre pessoas conversando com pessoas. Não previ algo importante: o aspecto de rede social da Internet — conta Kleinrock. — Eu não percebi que minha mãe de 99 anos estaria na Internet ao mesmo tempo que minha neta, de 7 (MATSUURA, 2019).

era um mero estudante de pós-graduação no MIT, entre 1960 e 1962. Ele desenvolveu a teoria matemática de redes de pacotes, a tecnologia subjacente à Internet, uma teoria que mais tarde seria chamada de comutação de pacotes, em que a informação seria transformada em pequenos pacotes eletrônicos antes de ser enviada para outro computador (OLIVEIRA, 2011, p.23).

Na mesma época, o engenheiro Paul Baran, da RAND Corporation, uma organização criada no final da Segunda Guerra Mundial para assessorar a Força Aérea norte-americana, também demonstrou a viabilidade da comutação de pacotes eletrônicos digitais, cada mensagem seria dividida em uma série de mensagens curtas, pedaços de comprimento fixo, e cada um seria enviado como um pacote endereçado individualmente que encontraria seu próprio caminho por meio da rede por qualquer rota que estivesse disponível, saltando de nó em nó até chegar ao ponto final do destino. Se partes da rede fossem destruídas, a autossuficiência de cada nó mais os dados dentro do pacote permitiriam que o nó buscasse formas alternativas de mover o pacote até o destino final (RAND, 1996, p.33).

> O Projeto RAND – uma organização formada imediatamente após a Segunda Guerra Mundial para conectar o planejamento militar com decisões de pesquisa e desenvolvimento – separou-se da Companhia Aérea Douglas de Santa Monica, Califórnia, e tornou-se uma organização independente e sem fins lucrativos. Adotando seu nome de uma contração do termo pesquisa e desenvolvimento, a entidade recém-formada dedicou-se a promover trabalhos de fins científicos, educacionais e de caridade para o bem-estar e segurança do cidadão americano (RAND, 2024).

Os conceitos de comutação de pacotes foram originados, de forma simultânea e independente, por pesquisadores dos Estados Unidos e da Inglaterra (CARVALHO, 2006, p.12). Donald Davies, do Laboratório Nacional de Física (*National Physical Laboratory* - *NPL*) do Reino Unido, coordenou, no início dos anos 1960, um projeto de redes de comunicação de computadores financiado pelo governo britânico. Foi ele quem deu o nome *packet* (pacote) ao sistema em um memorando do NPL em junho de 1966 (OLIVEIRA, 2011, p.23).

> Em 1947, Donald Davies após aprender sobre o Automatic Computing Engine (ACE), se juntou ao laboratório National Physical Laboratory (NPL) como membro de uma pequena equipe, liderada por Alan Turing, famoso por Bletchley Park. O trabalho do grupo, baseado no projeto de Turing, eventualmente levou ao desenvolvimento do computador Pilot ACE. Foi um dos primeiros quatro ou cinco computadores digitais com programas armazenados eletrônicos do mundo. Davies desempenhou um papel importante no projeto e no desenvolvimento da máquina e de seu sucessor, o ACE em grande escala. Em 1966, regressou ao NPL e envolveu-se no desenvolvimento de uma ideia que originou em 1965: para conseguir a comunicação entre computadores era necessário um serviço de comunicação de troca rápida de mensagens, no qual mensagens longas eram divididas em pedaços e enviadas separadamente para minimizar o risco de congestionamento. Os

> pedaços ele chamou de pacotes, e a técnica ficou conhecida como comutação de pacotes. A Agência de Projetos de Pesquisa Avançada da América (ARPA) e a ARPANET receberam seu projeto de rede com entusiasmo e a rede local NPL se tornou as duas primeiras redes de computadores do mundo a usar a técnica (SOCIETY, 2023a).

O IPTO seguia firme com a sua decisão de montar uma rede que interligasse os computadores das instituições financiadas (CARVALHO, 2006, p.15). Para gerenciar esse projeto, em 1966, Taylor recrutou Lawrence Roberts, gerente de programa do Laboratório Lincoln (*Lincoln Lab*) do MIT, no qual trabalhara em um projeto (também financiado pela ARPA) de interconexão entre computadores através de linhas telefônicas e também para supervisionar o desenvolvimento do ARPANET. Roberts vinha realizando experimentos de rede na Lincoln Lab, e Taylor o considerou o candidato mais qualificado para gerenciar o projeto ARPANET (ABBATE, 2000, p.44).

> Roberts inicialmente relutou deixar seu cargo de pesquisador. As circunstâncias de sua adesão ao IPTO forneceram um exemplo da influência da ARPA sobre a comunidade de pesquisa da ciência da computação. Quando Roberts recusou um convite inicial vir para a ARPA, Taylor pediu ao diretor da ARPA, Charles Herzfeld, que ligasse para o chefe do Laboratório Lincoln para lembrá-lo de que metade dos recursos de seu laboratório, que o financiamento veio da ARPA (ABBATE, 2000, p.44).

Em 1968, os pesquisadores da ARPA, sob a coordenação de Lawrence Roberts e Robert Taylor, concederam um contrato à Bolt, Beranek e Newman (BBN), uma empresa formada por professores e alunos do MIT, para construir uma rede de teste que seria conhecida como ARPANET, a predecessora da Internet (OLIVEIRA, 2011, p.23). Os projetistas da ARPANET ainda não tinham um plano específico sobre como as funções seriam divididas em camadas, muito menos de como as interfaces e protocolos de comunicação iriam funcionar. Essas definições foram acontecendo ao longo do tempo, na medida em que a rede foi se desenvolvendo (CARVALHO, 2006, p.17).

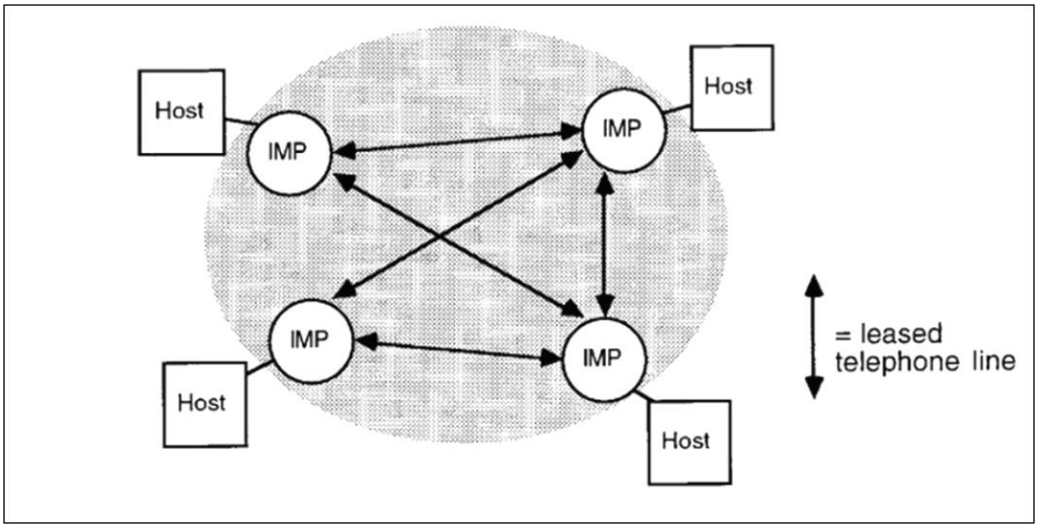
Uma das primeiras preocupações foi em relação à necessidade de criação de software de roteamento de pacotes para cada um dos diferentes sistemas operacionais que eram usados nos computadores das instituições (CARVALHO, 2006, p.17). Para transpor esse problema houve a participação de pesquisadores de outras universidades, inclusive com a presença de Kleinrock, para desenvolverem um sistema chamado de Interface Message Processor (IMP) cuja finalidade era permitir a comutação de pacotes de dados entre computadores de fabricantes diferentes (OLIVEIRA, 2011, p.23).

A Rede ARPA foi projetada desde o princípio para que cada nó recebesse uma cópia da mensagem e se mantivesse armazenada até que a mensagem fosse recebida com segurança no próximo nó. A rede funcionaria como um sistema de armazenamento e

encaminhamento e como tal deveria lidar com problemas de roteamento, *buffer*, sincronização, controle de erros, confiabilidade e outras questões relacionadas. Para isolar os centros de informática desses problemas e para isolar a rede dos problemas dos centros de informática, a ARPA decidiu colocar pequenos processadores idênticos em cada nó da rede para interconectar esses pequenos processadores com circuitos das operadoras telefônicas alugados para formar uma sub-rede (vide figura 1), e conectar cada centro de informática de pesquisa à rede através do pequeno processador local. Neste arranjo os centros de pesquisa em informática foram chamados de *Hosts* (hospedeiros) e os pequenos processadores foram chamados de processadores de interface de mensagem (HEART et al., 1970, p.551).

A equipe ARPANET começou a ver o sistema dividido conceitualmente em duas camadas: uma camada de comunicações, consistindo em IMPs de comutação de pacotes conectados por linha telefônica e uma camada hospedeira, que coordenaria as interações entre hospedar processos e fornecer serviços ao usuário, conforme demonstrado na figura 2 (HEART et al., 1970, p.551).

Figura 1 - Modelo de Rede com sub-redes de comunicações



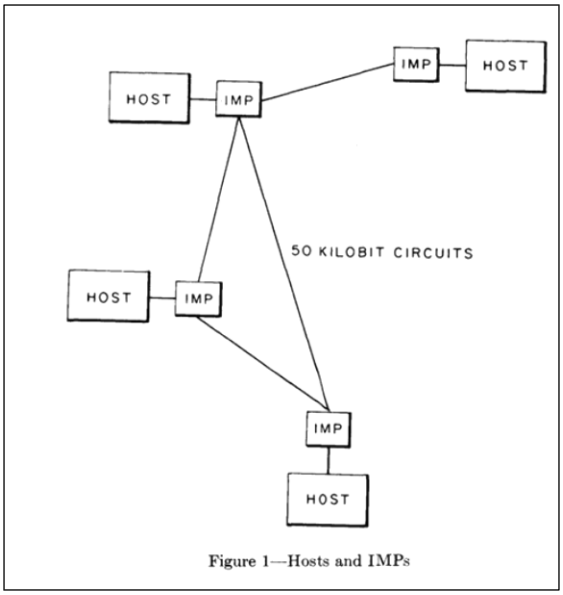
Fonte: (ABBATE, 2000, p.52)

A seguir, o modelo proposto de duas camadas da ARPANET

Nome da Camada	Funções
Host	Lida com a interface do usuário; inicia e mantém conexões entre pares de hosts.
Comunicações	Move dados pela sub-rede usando comutação de pacotes; garante transmissão confiável do host para IMP e de conexões IMP-IMP.

Fonte: (ABBATE, 2000, p.53)

Figura 2 – Hosts e IMPs



Fonte (HEART et al., 1970, p.552)

Em setembro de 1969 foi instalado o primeiro host da futura rede na UCLA (Universidade da Califórnia em Los Angeles), no laboratório de Leonard Kleinrock. O segundo computador foi conectado no Instituto de Pesquisa de Stanford (SRI), em Menlo Park, também na Califórnia, a cerca de 560 quilômetros de distância (HAFNER; LYON, 1998).

Durante semanas, os pesquisadores da UCLA se prepararam para sua primeira sessão de login discando para o sistema SRI de longa distância para se familiarizarem com o sistema de compartilhamento de tempo (*time-sharing*) do SRI. Com ambos os IMPs instalados e ambos os hosts em execução, o momento de testar os dois nós se tornou possível. O teste final da ARPANET se demonstrou viável (HAFNER; LYON, 1998).

A primeira conexão aconteceu no dia 29 de outubro de 1969[7], às 22h30, com uma mensagem que partiu do laboratório de Kleinrock na UCLA para o SRI em Stanford. A figura 3 mostra o primeiro roteador de pacotes para a ARPANET. A figura 4 aparece Kleinrock no laboratório onde a Internet surgiu, a seguir um pequeno relato de Kleinrock como isso aconteceu:

> Eu estava supervisionando o estudante-programador Charley Kline e nós fizemos a transmissão da mensagem do computador Host SDS Sigma 7 para o computador Host SDS 940 da SRI. A transmissão era simplesmente para fazer o login [código de acesso] para a SRI com a equipe do professor Engelbart. Nós tivemos sucesso em transmitir o 'l' e o 'o' e então o sistema caiu. Por isso, a primeira mensagem na Internet foi 'lo'[olhe]. Nós estávamos aptos para fazer o login total uma hora mais tarde" (OLIVEIRA, 2011, p.24).

Figura 3 –Processador de Interface de Mensagens foi o primeiro roteador de pacotes para a ARPANET

Fonte: (RICHARDS, 1965)

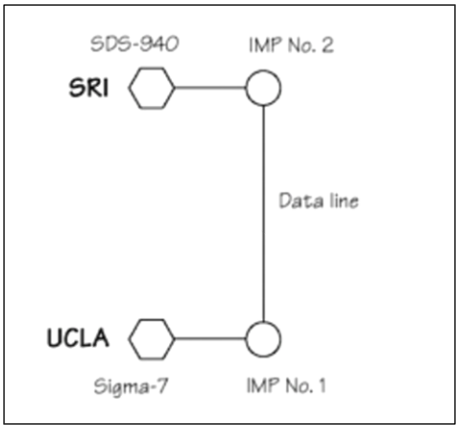
[7] No caso da Internet há outra coincidência reveladora: em agosto de 1969, mesmo ano do nascimento" da Internet, houve o Woodstock, o famoso festival de música em Bethel, no estado de Nova Iorque, EUA. E em 1969 o homem chegava à lua: "um pequeno passo para o homem, e um salto gigantesco para a humanidade". Também em 1969, enquanto a contracultura florescia em diversos estados norte-americanos, como o da Califórnia, na China a revolução cultural atingia seu ápice. Ou seja, 1969 não foi trivial...(GETSCHKO *apud* DEMENTSHUK; HENRIQUES, 2019)

Figura 4 - Leonard Kleinrock no laboratório das primeiras mensagens enviadas da Internet

Fonte: (MATSUURA, 2019)

Uma rede agora existia. A primeira rede da ARPA tinha o esquema parecido com isso:

Figura 5 - Primeira rede da ARPA

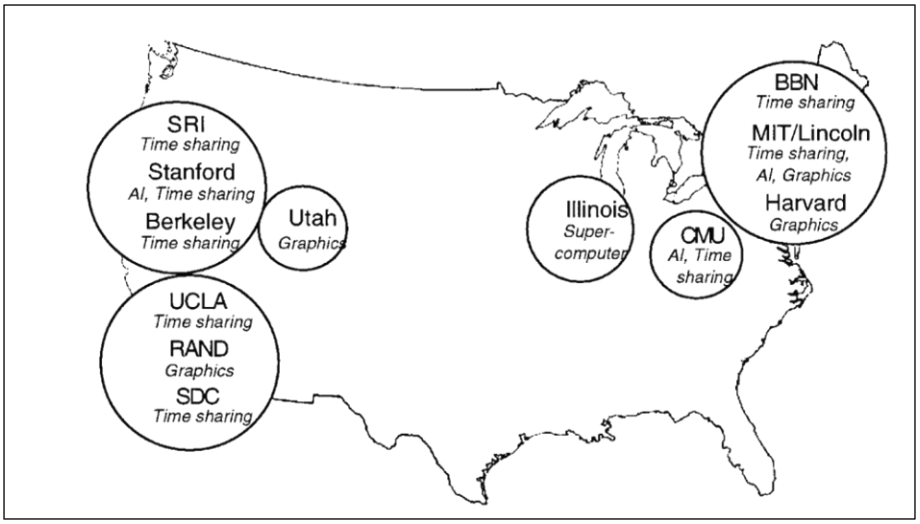


Fonte: (HAFNER; LYON, 1998)

A figura 5 mostra o esquema de ligação da primeira rede da ARPA. Posteriormente, em novembro uma nova rede foi conectada, o IMP número três foi instalada na Universidade Californiana de Santa Bárbara (UCSB), o quarto IMP foi na cidade Salt Lake City, na Universidade de Utah. A ARPANET começou como uma rede com quatro grandes computadores e uma velocidade de 2,4 kilobits por segundo (kbps), que logo subiu para 50 Kbps, após acordo com as companhias telefônicas proprietárias

das linhas que sustentavam a rede (OLIVEIRA, 2011, p.24). A figura 6 mostra a expansão da interligação das sub-redes nos Estados Unidos.

Figura 6 - Os principais centros de pesquisa do IPTO na época da criação da ARPANET

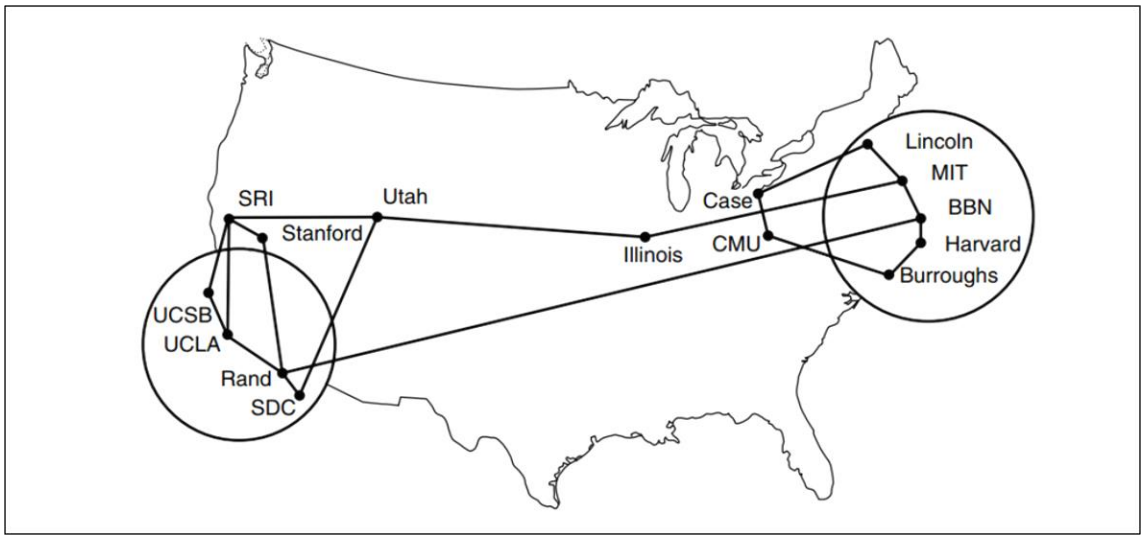


Fonte: ABBATE, p.45

O desenho da rede permitia a conexão de sites (*host)* adicionais. Um mapa de uma rede projetada em janeiro de 1971 já com quinze nós, figura 7. O mapa a seguir, figura 8, projeta a ARPANET em 1977, com diversos nós interligados em diferentes regiões dos Estados Unidos, assim como dois circuitos via satélite, um conectado a Londres e outro no Havaí.

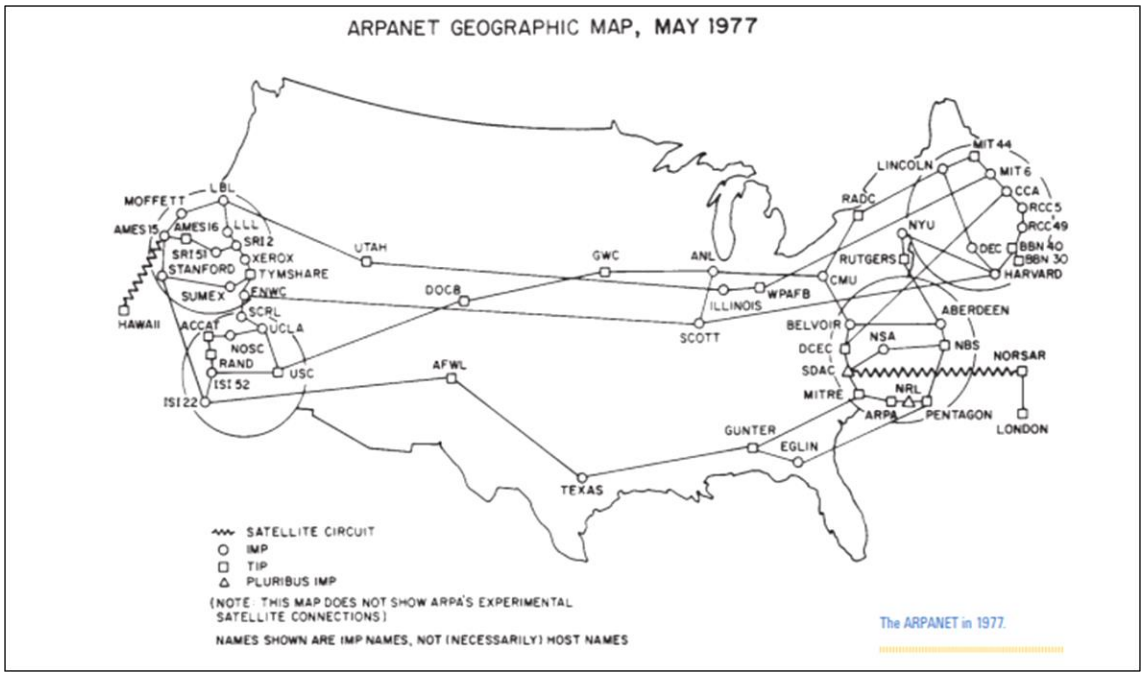
> A rede se expandiu rapidamente, incluindo computadores de variadas plataformas de *hardware* e de *software*, demonstrando que a comunicação e cooperação entre sistemas até mesmo de concepções muito diferentes era perfeitamente factível. Havia 13 computadores na rede em janeiro de 1971, 23 em abril de 1972 e 38 em janeiro de 1973. Foi organizada a primeira demonstração pública da rede em 1972 por ocasião da ``*First International Conference of Computer Communications''*, realizada no outono de 1972. Nesta oportunidade a rede já dava suporte a um amplo conjunto de serviços regulares, entre as quais estavam incluídos o login remoto e o correio eletrônico, cujo volume de uso surpreendeu os próprios responsáveis pela rede. Ou seja, a rede estava se revelando, desde os seus primórdios, como um instrumento muito efetivo de cooperação (SIMON, 1997a).

Figura 7 - Um mapa de 15 nós da ARPANET em 1971



Fonte: ABBATE, p.45

Figura 8 – Mapa Geográfico da Arpanet em 1977



Fonte:(KENYON, 2018, p.105)

A ARPANET estava então concebida e testada como uma rede de comunicação descentralizada, sem uma central de operações. A ideia era pensar na possibilidade de um ataque, ou seja, de quatro computadores, se dois não funcionassem em um ambiente de guerra, por exemplo, os outros dois poderiam se comunicar. A princípio, por se tratar de um contexto de Guerra Fria e de segurança, a ARPANET ficou restrita a alguns institutos

de pesquisa governamentais e universidades. Mas isso não impediu que ela extrapolasse a esfera militar e científica, com o seu uso também para a troca de mensagens pessoais (OLIVEIRA, 2011, p.24).

A cultura organizacional em torno da ARPANET era notavelmente descentralizada, acadêmica e informal. Ao coordenar seus contratantes, a DARPA dependeu em grande parte de acordos colaborativos em vez de contratos e obrigações. As decisões técnicas eram geralmente tomadas por consenso (ABBATE, 2000, p. 54).

A própria rede proporcionou uma nova forma de coordenar atividades dispersas e passou a funcionar como um ponto de encontro para a comunidade da ciência da computação. Embora às vezes surgissem conflitos entre os idealizadores, a cultura ARPANET melhorou a capacidade da DARPA de conseguir o apoio da comunidade científica e responder aos desafios técnicos que o projeto representava (ABBATE, 2000, p.54).

Em 1973, os pesquisadores apoiados pela DARPA tinham apresentado quatro tecnologias de comutação de pacotes (como pacotes de rádio e pacotes de satélite), o que levou ao próximo desafio: como desenvolver padrões que permitissem que essas tecnologias comunicassem entre si (KENYON, 2018, p. 105).

Vinton Cerf, que estava na Universidade Stanford na época e trabalhava sob contrato para a DARPA, explicou que demorou cerca de seis meses de trabalho para desenvolver a arquitetura correta e criar um protocolo aproximado. Ele e Robert Kahn, então diretor do IPTO da DARPA, que em 1976 contratou Cerf como gerente de programa, começaram trabalhar no que se tornaria o Protocolo de Controle de Transmissão (*Transmission Control Protocol* - TCP) e o protocolo da Internet (Internet Protocol - IP) (KENYON, 2018, p.105).

A implementação inicial do primeiro protocolo TCP/IP[8] ocorreu em Stanford em 1975. Conforme foi testado nos anos seguintes, o então famoso protocolo estava sendo

[8] De uma forma simples, o TCP/IP é o principal protocolo de envio e recebimento de dados da Internet. TCP significa Transmission Control Protocol (Protocolo de Controle de Transmissão) e o IP, Internet Protocol (Protocolo de Internet). O protocolo é uma espécie de linguagem utilizada para que dois computadores consigam se comunicar. Por mais que duas máquinas estejam conectadas à mesma rede, se não "falarem" a mesma língua, não há como estabelecer uma comunicação. Então, o TCP/IP é uma espécie de idioma que permite às aplicações conversarem entre si. Na realidade, o TCP/IP é um conjunto de protocolos. Esse grupo é dividido em quatro camadas: aplicação, transporte, rede e interface. Cada uma delas é responsável pela execução de tarefas distintas. Essa divisão em camadas é uma forma de garantir a integridade dos dados que trafegam pela rede (MARTINS, 2012).

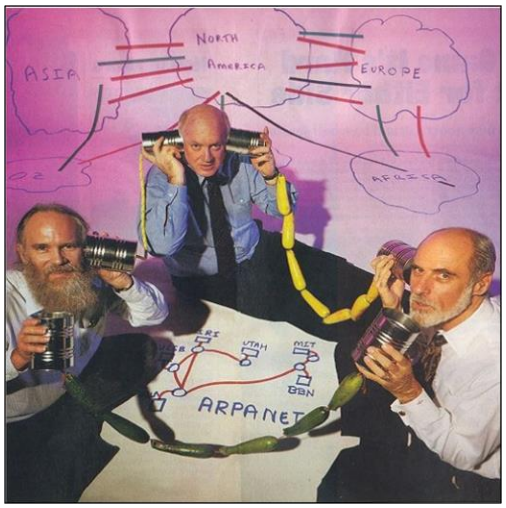
implementado em um número crescente de computadores operando sistemas em todo o mundo. Em janeiro de 1983, um número suficiente de redes individuais se conectou entre si, o que possibilitou a expansão da ARPANET para a Internet. Em 1990, a ARPANET original foi formalmente desativada. (KENYON, 2018, p.105).

> Depois de vários experimentos realizados com o novo protocolo, o Departamento de Defesa resolveu que, em janeiro de 1983, todos os computadores da Arpanet deveriam mudar para o TCP. Com a Arpanet fechada para poucos, algumas universidades norte-americanas queriam ter uma rede própria. Em 1979, essas universidades ganharam o apoio da *National Science Foundation* (NSF), dos Estados Unidos. Dois anos depois, com um orçamento de US$ 5 milhões, começou a funcionar a *Computer Science Network* (CSNet) reunindo grupos de pesquisa de computação que estavam fora da Arpanet. A nova rede usou o TCP/IP e foi a primeira a ter conexão com a Arpanet. A CSNet foi mantida pela NSF por um período de três anos, depois se tornou independente. Sem a CSNet, a NSF planejou uma nova rede mais ampla que pudesse abranger não apenas os estudiosos em computação e transformá-la em uma ferramenta para a pesquisa acadêmica, inclusive fornecendo a tecnologia para qualquer pessoa dentro da universidade, e não apenas para os pesquisadores. A instituição lançou em 1986 a NSFNet com o objetivo de interligar redes, a "inter net", como foi escrito ou fazer uma rede de redes. A NSFNet começou suas atividades utilizando o TCP/IP a uma velocidade de 56 kbps. Ela estimulou redes regionais nos Estados Unidos e montou uma estrutura de conexões de Internet no país. No início dos anos 1990, a maioria das redes, como a Bitnet e a CSNet, passou a ser roteada para a Internet, demonstrando a versatilidade do sistema. Nesse ponto, os militares resolveram criar a sua própria rede, a Milnet, e a Arpanet foi extinta. Nos anos seguintes, outros países aderiram à NSFNet e ocorreu um aumento sem precedentes que fez crescer os olhos de quem estava fora das redes acadêmicas ou saía da universidade e sentia falta delas. Assim, em 1991, a NSF permitiu o uso da rede para fins comerciais e a partir de 1995 transferiu sua estrutura para a iniciativa privada (OLIVEIRA, 2011, p.25).

Na fotografia a seguir (figura 9), publicada no dia 08 de agosto de 1994 na revista Newsweek, para comemorar os 25 anos de aniversário da ARPANET, aparecem as figuras de Jon Postel, Steve Crocker[9] e Vint Cerf. Eles seguravam embalagens de comida enlatada, como se fossem bocais de telefone, interligados por abobrinhas verdes e abóboras amarelas. Observa-se que a rede não podia funcionar “pois não havia uma boca e ouvido em nenhuma das conexões”. Essa era a representação da ARPANET nos primórdios dos anos 60, antes do protocolo TCP/IP estar estabelecido. O que simbolizava várias instituições americanas com os seus computadores conectados, mas sem comunicação entre as redes, cada um utilizava uma linguagem diferente.

[9] Dr. Crocker estava envolvido na Internet desde o seu início. No final da década de 1960 e início da década de 1970, enquanto era estudante de graduação na UCLA, fez parte da equipe que desenvolveu os protocolos para a ARPANET e lançou as bases para a Internet de hoje. Ele organizou o Grupo de Trabalho de Rede, que foi o precursor da moderna Força-Tarefa de Engenharia da Internet e iniciou a série de notas *Request for Comment* (RFC) por meio das quais os projetos de protocolo são documentados e compartilhados. Por este trabalho, o Dr. Crocker recebeu o Prêmio IEEE Internet de 2002 (SOCIETY, 2023b).

Figura 9 - Comemoração de 25 anos com os fundadores da ARPANET



Fonte: (CERF, 1994)

À medida que tecnologias como o TCP/IP melhoraram as redes, cientistas e os engenheiros começaram a prestar atenção em outros sistemas de suporte, como exibições gráficas (KENYON, 2018, p.105). Antes de a Internet tornar-se aberta a todos, outra tecnologia surgiu para fortalecê-la. Em 1989, ocorreu o nascimento da *World Wide Web* (WWW), ou simplesmente Web, nos laboratórios da Organização Europeia de Pesquisas Nucleares, conhecida como CERN, localizada na Suíça (OLIVEIRA, 2011, p.25). Ela foi concebida pelo britânico Timothy Berners-Lee[10], físico por formação e engenheiro de software por vocação e profissão, pesquisador da instituição, que estudava um sistema para trocar documentos científicos entre instituições ligadas ao CERN existentes em várias partes do mundo. Segundo Carvalho (2006, p.127), é comumente apresentado como o gênio que, após momento de mágica inspiração, criou a Web, tão utilizada atualmente. Entretanto, essa atribuição de mérito é refutada pelo próprio autor:

> Os jornalistas sempre me perguntam qual era a ideia crucial, ou qual foi o evento singular que permitiu a existência da Web de um dia para o outro. Eles ficam frustrados quando digo que não houve um momento tipo “Eureka!”. Não foi como a lendária maçã caindo na cabeça de Newton para demonstrar o conceito de gravidade. A invenção da World Wide Web envolveu minha crescente percepção de que havia um poder em organizar ideias de uma maneira não restritiva e semelhante a uma teia. E essa consciência veio até mim precisamente por esse tipo de processo. A Web surgiu como resposta a um desafio aberto, através de um turbilhão de influências, ideias e realizações de muitos lados, até que, pelos assombrosos ofícios da mente humana, um novo conceito se consolidou. Isto

[10] Sir Tim foi nomeado uma das 100 pessoas mais importantes do século XX pela revista Time e em 1989 escreveu um memorando chamado 'Gestão de Informação: Uma Proposta', no qual unificou o hipertexto com a Internet para criar um sistema de partilha e distribuição de informação. globalmente. Ele também criou o primeiro navegador, servidor e editor, e garantiu que a tecnologia fosse disponibilizada gratuitamente para todos (OXFORD, 2016).

> foi um processo por etapas, e não uma solução linear de um problema bem definido após o outro (BERNERS-LEE, 1999, p.03).

No entanto, Berners-Lee não atuou sozinho para a criação da Web, teve apoio de um grande parceiro empreendedor, Robert Cailliau, um físico belga que também trabalhou no CERN. Para Berners-Lee, o verdadeiro dom de Robert era o entusiasmo, um gênio da evangelização. Enquanto Berners ficava sentado escrevendo códigos, Robert, cuja sala era perto da dele, colocava suas energias para desenvolver o projeto WWW no CERN. Cailliau era um "cientista-empresário" que fazia lobby por meio de sua extensa rede de amigos espalhada por toda a organização, o que incluía estudantes, dinheiro, máquinas e salas (BERNERS-LEE, 1999, p.26).

Juntos apresentaram, em 1990, o protocolo de transferência de hipertexto (HTTP, na sigla em inglês) e a linguagem de marcação de hipertexto (HTML), um software para desenho de páginas na web (OLIVEIRA, 2011, p.25).

> O HTTP é também um protocolo baseado no TCP/IP. Como tudo na Internet, o crescimento foi muito rápido. Contou muito para essa expansão o fato de o Cern e Berners-Lee não solicitarem uma patente do invento. Com o sistema HTTP difundido, pesquisadores do Centro Nacional de Supercomputação e Aplicações, da Universidade de Illinois, campus de Urbana-Champaign, nos Estados Unidos, criaram o Mosaic em 1993, o primeiro navegador da web com as informações posicionadas de forma gráfica que depois originou o Netscape, o primeiro comercial, que difundiu a web para todo o planeta (OLIVEIRA, 2011, p.25).

Cailliau (2013) conta que em algum momento de 1992, quando ainda havia poucos servidores web no mundo (menos de 50), Tim Berners-Lee e ele pensavam em como espalhar a WWW para todo o mundo. Até aquele momento, os direitos pertenciam ao CERN, e a tendência era que as universidades patenteassem as suas invenções e ganhassem dinheiro com elas. Existiam vários modelos, sendo um deles pedir *royalties* por cada instalação do software. Havia também a possibilidade de tentar comprar os direitos do CERN por uma quantia fixa, sair e montar uma empresa baseada na *World Wide Web* (WWW).

Houve muitas discussões e até diversas propostas de preços. Mas a experiência do *Gopher*, um protocolo de redes de computadores que foi desenhado para distribuir, procurar e acessar documentos na Internet, não foi encorajador: quando a Universidade de Minnesota começou a cobrar *royalties*, o uso do Gopher estagnou.

> Pela minha experiência anterior, estava mais inclinado a abrir uma empresa. Tim me perguntou se eu queria ser rico. Eu realmente não tinha pensado nisso como o objetivo de um negócio, mas respondi que ajudaria. Tivemos algumas sessões de brainstorming mais sérias sobre o status da WWW, mas no final algumas coisas ficaram claras: o que tínhamos não era um "aplicativo" patenteável e sofisticado, tínhamos padrões (html, http)

> e alguns pedaços de software que faziam uso desses padrões, mas nada espetacular. Havia também um bom número de redes de conteúdo altamente desenvolvidas já em funcionamento, várias nos EUA, várias na Europa. Estaríamos competindo com eles, e fazendo isso em uma plataforma chamada Internet, da qual ninguém fora da academia tinha ouvido falar muito (CAILLIAU, 2013).

Em termos gerais, a escolha estava entre licenciar o software sob condições comerciais restritivas ou disponibilizar gratuitamente o software WWW, seguindo o espírito da Convenção CERN. Segundo Cailliau, levou-se um tempo para a tomada de decisão, pois os argumentos eram complexos e não estava claro o que aconteceria com a WWW em ambos os casos. Por fim, com a intenção de se fazer algo útil, mais do que enriquecer, decidiu-se usar o modelo tradicional do CERN para *spin-off*[11] de tecnologia: torná-la disponível gratuitamente. Mesmo com o conceito de licenciamento *Open Source* ainda incipiente, optaram por colocar o software WWW no domínio público, renunciando aos direitos de propriedade intelectual do CERN sobre o WWW (CAILLIAU, 2013).

Para oficializar esta decisão, ou seja, publicar um documento legal confiável, exigiu-se uma estreita colaboração com o Serviço Jurídico do CERN. No dia 30 de abril de 1993, o documento foi assinado. Pode-se considerar a WWW um hipertexto de formato simples, mas de possibilidade de ampliação indefinida, pois é baseada em texto e é guiada por padrões abertos e livres onde qualquer um pode contribuir. O fato de a CERN ter disponibilizado o software da WWW logo no início de sua criação para o domínio público foi um dos fatores de sucesso para que a Internet transcendesse ao mundo acadêmico, militar ou das grandes empresas de tecnologia (CAILLIAU, 2013).

1.3. Internet no Brasil

Por volta de 1985, Demi Getschko, o então superintendente do Centro de Processamento de Dados da FAPESP[12], relatou que havia muita pressão pela conexão e

[11] O termo Spin-off é bastante comum na área do cinema, das séries e até da música. Por exemplo, um personagem secundário pode se destacar tanto a ponto de um filme posterior ser feito apenas para contar a sua história. A ideia foi aplicada a empresas durante a década de 1960, com os centros de pesquisa do Vale do Silício, na Califórnia. Dessa forma, a Spin-off também se mostrou uma estratégia muito vantajosa para empreendedores. Afinal, trata-se da criação de uma nova empresa ou produto, a partir do seu negócio atual (KUVIATKOSKI, 2022).

[12] Fundação de Amparo à Pesquisa do Estado de São Paulo é uma das principais agências de fomento à pesquisa científica e tecnológica do país. Com autonomia garantida por lei, a FAPESP está ligada à Secretaria de Ciência, Tecnologia e Inovação do Estado de São Paulo. Com um orçamento anual correspondente a 1% do total da receita tributária do Estado, a FAPESP apoia a pesquisa e financia a investigação, o intercâmbio e a divulgação da ciência e da tecnologia produzida em São Paulo (FAPESP, 2023).

troca de informações, principalmente na área acadêmica, e que, devido ao crescimento da Internet nos Estados Unidos, não seria surpresa a posterior chegada da Internet no Brasil. No entanto, a demanda pela conexão de estudiosos de outros países fez com que a FAPESP se voluntariasse para conseguir uma conexão que atendesse as universidades estaduais e também os institutos de pesquisas IPT (PRACIANO, 2019).

> Com a missão definida, Getschko e os demais pesquisadores começaram a ver como fariam esta história e descobriram que uma das redes fáceis de usar lá fora, que todo mundo estava usando era a BitNet, uma rede boa para correio eletrônico. Correio eletrônico, frisa o cientista brasileiro, era uma ferramenta de extrema popularidade na época. "Era muito séria, pois o cara podia ser o maior figurão que acabava respondendo", pontua (PRACIANO, 2019).

A entrada da Internet na Fundação ocorreu por meio de uma conexão direta com o laboratório FERMILAB, especializado em física de altas energias e de partículas atômicas, situada na cidade de Batavia, em Illinois, nos Estados Unidos. Essa conexão permitia que pesquisadores brasileiros acessassem as informações e os contatos com seus pares naquela instituição e em outras partes do país norte-americano e europeu por meio de uma das predecessoras da Internet, a BITNET[13] (OLIVEIRA, 2011a, p.17).

> A conexão funcionava via linha telefônica ponto a ponto sem necessidade de discagem, por um fio de cobre dentro de um cabo submarino, porque ainda não havia fibra óptica para esse tipo de serviço. Ela era operada pela Academic Network at São Paulo, a ANSP, a rede acadêmica de São Paulo, criada e mantida financeiramente pela FAPESP desde 1988 para suprir a comunicação eletrônica entre as principais instituições de ensino e pesquisa paulistas (OLIVEIRA, 2011a, p.17).

Para Oliveira (OLIVEIRA, 2011a, p.17), a Internet chegou ao Brasil sem "pompas, banda de música ou discurso", em um dia incerto de janeiro de 1991, no início do período tradicional de férias da FAPESP, na sede da Fundação no bairro da Lapa, em São Paulo. Segundo Simon (1997b), a ligação da FAPESP não foi a primeira conexão de rede a chegar ao Brasil. Ela foi precedida pelo Laboratório Nacional de Computação Científica - LNCC do Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq, situado em Petrópolis – RJ, que alugou uma linha da Embratel três meses antes da FAPESP, com objetivo de conectar com a Universidade de Maryland via BITNET (PRACIANO, 2019). Na mesma época, a Universidade Federal do Rio de Janeiro (UFRJ) também se conectou à Internet através de links com universidades americanas (VIEIRA, 2003). Mas a linha da LNCC, embora muito importante, não teve a sorte de ter o mesmo impacto da iniciativa da FAPESP. "A ligação do LNCC não evoluiu com o tempo e ela

[13] A Bitnet, sigla de Because It's Time Network, era muito usada por pesquisadores no exterior. Ela utilizava uma linguagem de computação criada pela empresa IBM (OLIVEIRA, 2011a, p.17).

foi desativada com a mesma velocidade inicial de 9.600 bps, em 1996, quando da desativação da rede BITNET no Brasil" (SIMON, 1997b).

De acordo com Getschko, foi na FAPESP que os "primeiros pacotinhos da Internet" começaram a trafegar em link de conexão. "Fomos a primeira conexão brasileira à Internet em janeiro de 1991 usando o protocolo TCP/IP que era o da Internet" (GETSCHKO *apud* PRACIANO, 2019). Por meio de acordos diretos com a administração das redes norte-americanas acadêmicas, Demi Getschko e a equipe do CPD da FAPESP conseguiram a delegação do domínio .br, que identifica o código do país nos endereços da web e dos e-mails (OLIVEIRA, 2014).

A experiência adquirida pela equipe da *Academic Network at São Paulo* - ANSP permitiu que a FAPESP, além de se tornar a conexão brasileira com a Internet, se transformasse no centro técnico do início da Internet brasileira. Esse advento possibilitou que a FAPESP servisse à Rede Nacional de Ensino e Pesquisa (RNP) criada pelo Ministério da Ciência e Tecnologia (OLIVEIRA, 2011a, p.20).

> A RNP foi criada em setembro de 1989; seu objetivo era construir uma infraestrutura nacional de rede de Internet de âmbito acadêmico. A Rede Nacional de Pesquisa, como era chamada em seu início, tinha também a função de disseminar o uso de redes no país (RNP, 2023).

A RNP serviria como forma de aglutinar as iniciativas que atendiam às diversas universidades. "Em vez de cada um tentar resolver seu problema, a RNP instalou uma *backbone* nacional que apontava onde cada instituição devia se conectar. E assim, a área acadêmica estava mais ou menos resolvida" (GETSCHKO *apud* PRACIANO, 2019).

> Backbone é a espinha dorsal da Internet — a coluna ou tronco de vários pontos de conexão. Como no corpo humano, um backbone conecta e sustenta os seus membros, aqui entendido como servidores distantes. A função do backbone em telecom é conectar as centrais das operadoras de Internet aos servidores externos (nacionais ou internacionais), geralmente de forma redundante e por rotas diferentes. Em resumo, trata-se de uma malha continental. Na prática, a estrutura é responsável pelo envio e recebimento dos dados entre diferentes computadores, dentro ou fora de um país. A rede principal (espinha dorsal) é dividida em outras para impedir que tráfego e transmissão de dados sejam lentos. Ou seja, seu computador faz parte de uma rede local, que está conectada à rede do seu provedor de Internet, que por sua vez se conecta a redes da sua cidade e a um backbone nacional que vai se conectar com redes internacionais via cabos submarinos (COSSETTI, 2023).

A RNP se formou em setembro de 1989 e já se preparava para se ligar à Internet em 1990, o que veio a acontecer entre 1991 a 1993, conhecida como fase 1, o que proporcionou acesso a várias instituições de pesquisa do país. Dessa primeira conexão, surgiu a primeira rede de Internet no Brasil, conectando dez estados e o Distrito Federal.

Ou seja, a princípio, o acesso à Internet tinha fins acadêmicos, para que pesquisadores brasileiros estivessem conectados entre si e com seus pares internacionais (RNP, 2023).

No dia 3 de junho de 1992, o Rio de Janeiro sediou a Conferência das Nações Unidas para o Meio Ambiente e Desenvolvimento, a Rio-92, o que criou as condições necessárias para a primeira conexão de Internet oficialmente realizada no país. A conferência reuniu chefes de estado e representantes de governo de cerca de 180 países, além de organizações não governamentais, cientistas, jornalistas e a sociedade civil para discutir a preservação ambiental e o desenvolvimento sustentável (RNP, 2022) e a definição de "medidas para enfrentar os problemas crescentes da emissão de gases causadores do efeito estufa" (BARRETO, 2009).

> Considerada um marco no debate sobre desenvolvimento sustentável, a Rio-92 atraiu os olhares do mundo inteiro e precisava de conexão internacional estável e de boa capacidade para acontecer. Na época, o setor de telecomunicações no Brasil era estatal e alegou não ter condições de prover acesso à Internet para a ocasião. Foi nesse momento que a RNP, até então um projeto do Ministério da Ciência e Tecnologia (MCT), articulou parcerias para realizar a entrega de uma infraestrutura de Internet para o evento (RNP, 2022).

Paralelamente ao início das operações da RNP, surgiu no Rio de Janeiro uma organização não governamental chamada Instituto Brasileiro de Análises Sociais e Econômicas (Ibase), que se tornaria a primeira instituição brasileira fora do ambiente acadêmico a utilizar a Internet, conhecida como Alternex[14] (VIEIRA, 2003). O grande teste do Alternex ocorreu em 1992, em um evento paralelo à Rio-92, o Fórum Global, onde representantes de ONGs se organizaram em tendas e discutiram medidas para lutas socioambientais. Durante o evento foi montado um sistema de veiculação de informações eletrônicas para acompanhar o andamento dos debates (RNP, 2022).

A fase 2 teve início a partir de 1994:

> "com o grande aumento de instituições conectadas à rede, ampliou-se a demanda sobre o backbone do Projeto. Paralelamente, percebeu-se que aplicações interativas não eram viáveis a velocidades inferiores a 64Kbps. Assim, o período de 1994 a 96 foi dedicado à montagem da Espinha Dorsal Fase II da RNP, com uma infraestrutura bem mais veloz que a anterior. A RNP firmou-se como referência em aplicação de tecnologia Internet no Brasil, oferecendo apoio ao surgimento e desenvolvimento de variadas iniciativas de redes estaduais. Em maio de 1995, teve início a abertura da Internet comercial no país. A RNP deixou de ser um backbone restrito ao meio acadêmico para estender seus serviços

[14] A Alternex era um sistema ("bulletin board system - BBS") por onde era possível consultar arquivos por uma base de dados e também se comunicar com usuários, inclusive com instituições no exterior, duas vezes por dia. O responsável pela Alternex, Carlos Afonso, articulou-se com o coordenador do projeto RNP, Tadao Takahashi (*in memoriam*), e dessa parceria, surgiram recursos do governo brasileiro para equipamentos que dariam suporte à infraestrutura necessária para os dois eventos, e que ficariam no país para o uso posterior (RNP, 2022).

> de acesso a todos os setores da sociedade. A capacidade de conexão internacional chegava a 4 Mbps" (RNP, 2009a).

A fase 3 ocorreu entre os anos de 1996 e 1998:

> "a RNP obteve consideráveis melhorias em sua infraestrutura, ampliando a capilaridade e velocidade de suas linhas. Com a evolução da Internet pública no Brasil e a multiplicação de provedores comerciais, a RNP pôde voltar-se novamente para a área acadêmica. A partir do lançamento do edital "Projetos de Redes Metropolitanas de Alta Velocidade" (Remavs), em outubro de 1997, a RNP deu início à terceira fase do projeto, denominada RNP2. Optou-se pelas Remavs porque havia, na época, uma carência de infraestrutura de fibras ópticas de alcance nacional. O objetivo era incentivar o desenvolvimento de uma nova geração de redes Internet, interligando todo o país numa rede de alto desempenho e conectando-se a outras iniciativas de redes avançadas no mundo. No final da década de 1990, os links do backbone com o exterior alcançavam 8 Mbps" (RNP, 2009a).

Utilização da tecnologia de transmissão *Asynchronous Transfer Mode* (ATM) – final da década de 90:

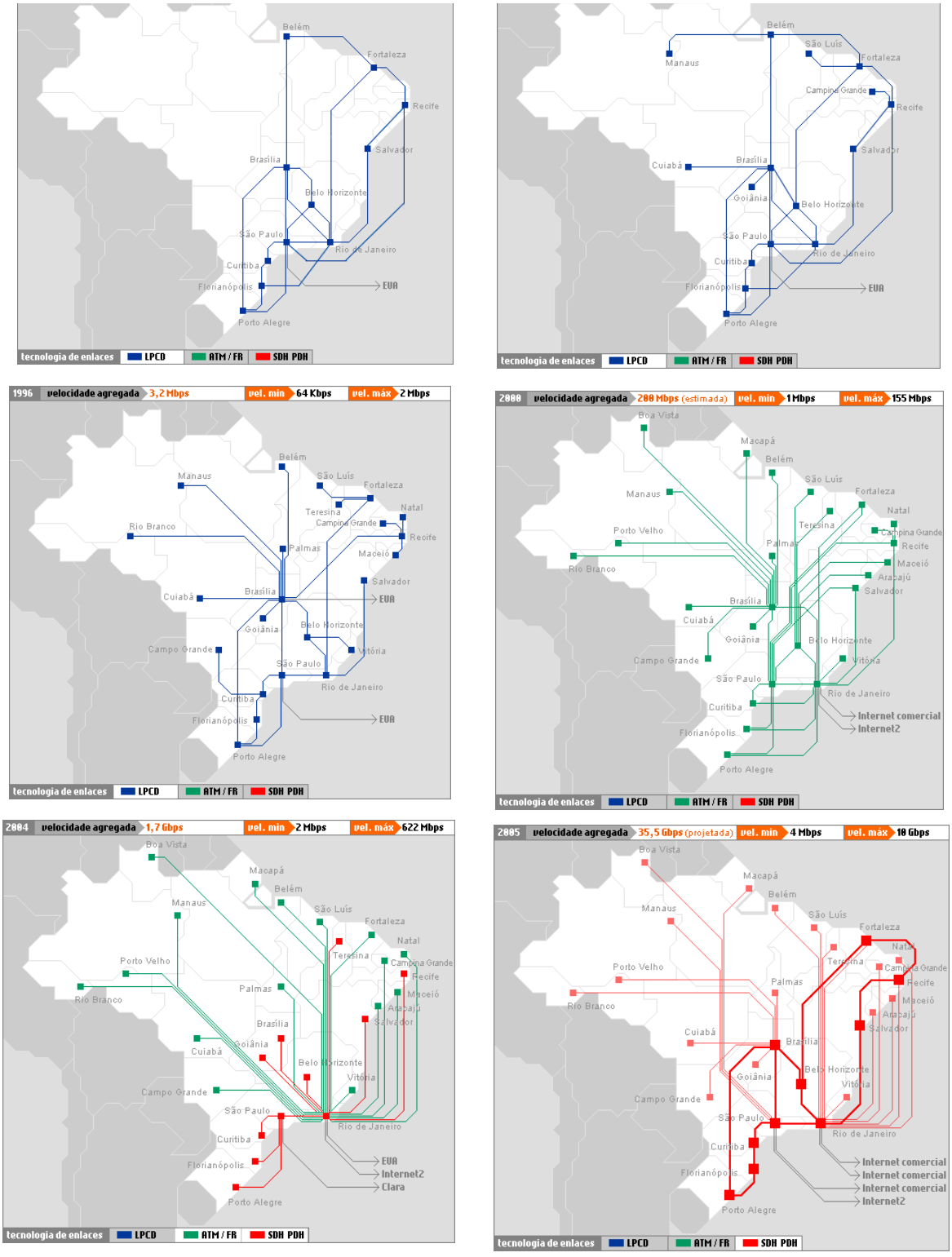
> Ao longo dos últimos anos da década de 1990, as operadoras de telecomunicação foram ampliando suas infraestruturas de fibras ópticas. Desta forma, em maio de 2000, o ministro da Ciência e Tecnologia, Ronaldo Mota Sardenberg, pôde inaugurar o novo backbone RNP2, o qual alcançava os 26 estados da federação e o Distrito Federal. Eram usadas as tecnologias de transmissão *Asynchronous Transfer Mode* (ATM) e *Frame Relay* (FR).
>
> Em fevereiro de 2001, a capacidade de tráfego internacional do RNP2 foi ampliada para 155 Mbps com a inauguração de um novo link com os Estados Unidos. Em agosto de 2001, foi ativado um canal de 45 Mbps entre o RNP2 e a rede do projeto Internet2, dos Estados Unidos. O enlace foi cedido pelo projeto *Americas Path Network* (Ampath), que integrou outras redes avançadas nos três continentes americanos.
>
> Uma nova conexão, desta vez com a portuguesa Rede Ciência, Tecnologia e Sociedade (RCTS), da Fundação para a Computação Científica Nacional (FCCN), foi estabelecida em fevereiro de 2002. O enlace, de 2 Mbps, possibilitou a realização de projetos conjuntos entre pesquisadores brasileiros e portugueses ao longo de mais de um ano. Foi desativado em 2003.
>
> Em 2004 a RNP integrou-se à Rede Clara (Cooperação Latino-Americana de Redes Avançadas), a qual se encontra conectada às redes avançadas da Europa e dos Estados Unidos. Nesta ocasião, foi desativado o link direto da RNP com a Internet2 (RNP, 2009a).

Substituição da tecnologia para *Synchronous Digital Hierarchy* (SDH*)* – março de 2004:

> A partir de março de 2004 os enlaces ATM e FR do *backbone* RNP2 começaram a ser substituídos por enlaces SDH (*synchronous digital hierarchy* ou hierarquia digital síncrona). A vantagem sobre o ATM é que os dados podem ser empacotados diretamente sobre este protocolo, o que não ocorria com a tecnologia ATM. Desta forma, cabem, na prática, mais dados em um canal com, teoricamente, a mesma capacidade. Os links interestaduais chegaram a 622 Mbps (RNP, 2009a).

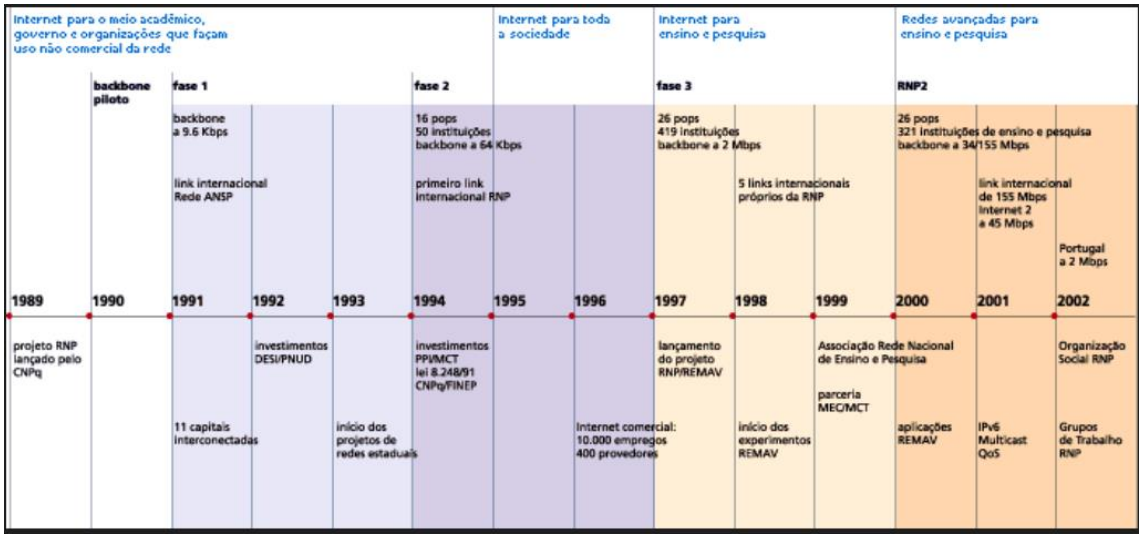
As figuras 10 e 11 demonstram a evolução do *backbone* e a linha do tempo da Internet brasileira.

Figura 10 – Evolução do *backbone* brasileiro



Fonte: (RNP, 2009a)

Figura 11 - Linha do Tempo da Internet brasileira



Fonte: (RNP, 2009b)

No dia 15 de maio de 1995, o Ministério de Ciência e Tecnologia (MCT) e o Ministério das Comunicações (MC) afirmaram em nota conjunta a necessidade de constituir um Comitê Gestor da Internet (CGI). No dia 31 de maio, a ANATEL publicou a Norma 4, que regula o uso de meios da Rede Pública de Telecomunicações para o provimento e utilização de Serviços de Conexão à Internet. Nesse mesmo dia, foi publicada a Portaria Interministerial nº 147 que criou o Comitê Gestor da Internet (CGI) no Brasil, formado por representantes da comunidade acadêmica, empresarial, provedores de serviços, usuários do serviço de Internet, CNPq, Sistema Telebrás, Ministério da Ciência e Tecnologia e das Comunicações. Uma das tarefas do CGI era acompanhar a disponibilização de serviços Internet no país e coordenar a atribuição de endereços IP (*Internet Protocol*) e o registro de nomes de domínios (.br) (CGI.br, [*s. d.*]).

Em setembro de 2003, o modelo de governança da Internet do Brasil foi publicado por meio do Decreto 4.829, com a atribuição de estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil e promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços de Internet, bem como para a sua crescente e adequada utilização pela sociedade, dentre outras (BRASIL, 2003).

Nessa nova reformulação do CGI, houve pequenas alterações de composição, tanto em número de conselheiros quanto na representação. Na configuração de 2003,

passou para 21 (vinte e um) membros, sendo 9 (nove) do governo e 11 (onze) da sociedade civil, eleitos pelos respectivos segmentos. Os nove do governo não têm prazo de mandato porque ficam até outro representante ser eventualmente nomeado pelo ministro correspondente (GETSCHKO *apud* OLIVEIRA, 2014).

> Às vezes, o próprio ministro é o ocupante da cadeira no CGI. Os 11 eleitos diretamente por suas comunidades têm três anos de mandato. Existem três assentos para a academia, quatro para o terceiro setor, quatro para a área empresarial, assim distribuídos: um para os usuários empresariais, um para provedores de acesso e serviços, um para provedores de infraestrutura e um para o segmento empresarial de software e hardware. Importante observar que o governo não tem maioria no CGI. O coordenador do CGI, por razões históricas, desde sua criação, é sempre o representante indicado pelo Ministério da Ciência, Tecnologia e Inovação. Em teoria teríamos uma situação em que 12 se sobrepõem aos nove numa votação, mas, em termos de Internet e de consenso, isso não seria nada bom. Uma votação com maioria apertada nunca aconteceu, a votação é, sempre que possível, substituída por comum acordo. Raramente tivemos votações e, quando houve, foi 20 a um, 19 a dois, por exemplo (GETSCHKO *apud* OLIVEIRA, 2014).

Getschko (*apud* OLIVEIRA, 2014) destaca a importância de manter o CGI sem o poder de imposição ou regulação, mas o de gerar bons normativos, tomar medidas, gerar estatísticas e oferecer cursos em áreas específicas a fim de contribuir com ações adequadas em favor da Internet no país.

Neste capítulo, observou-se que as evidências históricas demonstraram que a evolução dos computadores e da Internet tiveram o seu ápice de desenvolvimento após o fim da Segunda Guerra Mundial. O início da Guerra Fria e a bipolaridade política do mundo após o final do conflito impulsionaram o planeta para uma corrida armamentista e espacial entre as nações ditas como capitalistas e comunistas, principalmente Estados Unidos e a URSS. Esses fatores contribuíram para um aumento considerável no investimento em pesquisas científicas e na melhoria da educação. Tanto no exterior como no Brasil, verificou-se que foram as universidades, por meio dos seus centros de pesquisa, as precursoras na divulgação de trabalhos científicos e na implantação dessas novas tecnologias. Não só o setor militar se beneficiou como o funcionamento orgânico das sociedades como também passou a ser interdependente da tecnologia da informação e comunicações.

O que até então não se conhecia muito bem era que os malefícios tecnológicos poderiam ser usados para conflitos entre nações no espaço cibernético. O próximo capitulo relata quatro estudos de casos sobre conflitos cibernéticos, dois deles que envolveram duas nações no leste europeu, Estônia e a Georgia, um outro caso que trata

de um ataque cibernético a um alvo específico, na usina de enriquecimento de urânio no Irã e um último que envolveu um possível ataque ao setor energético brasileiro.

2. Quatro Estudos de Casos

A utilização do estudo de caso como estratégia de pesquisa atribui-se ao fato de ser um método que abrange situações diversas, com a lógica de planejamento incorporando abordagens específicas à coleta de dados. Para Robert Yin (2001, p.32-33) um estudo de caso é considerado uma investigação empírica que analisa um fenômeno contemporâneo dentro de seu contexto da vida real, ou seja, para a realização de uma pesquisa histórica certamente seria necessária a abordagem de situações emaranhadas entre fenômeno e contexto.

Cada um dos quatro estudos de casos apresentados nesta pesquisa histórica foi escolhido por se tratarem de situações relevantes no contexto histórico-cibernético. Os acontecimentos relatados, apesar de serem distintos entre si, formam um contexto único pois utilizaram do espaço cibernético para a conflagração de conflitos cibernéticos. As táticas, os métodos, os alvos, as consequências coletadas para alguns desses casos se assemelham em certos aspectos e a forma de análise possibilita que muitas das evidências históricas encontradas se convirjam para um ponto em comum: a cibersegurança.

2.1. Caso 1: Estônia (2007)

Estônia é um país localizado no nordeste da Europa (vide figura 12), o mais setentrional dos três estados bálticos, com uma população em torno de 1.418.000 habitantes (2024). A área da Estônia inclui cerca de 1.500 ilhas e ilhotas; as duas maiores destas ilhas, Saaremaa e Hiiumaa, ficam ao largo da costa oeste da Estônia continental. A parte terrestre projeta-se para o Mar Báltico, que circunda o país a norte e a oeste. A leste, a Estônia é limitada pela Rússia, predominantemente pelo rio Narva e pelos lagos Peipus, Tyoploye e Pskov - e ao sul é limitada pela Letônia (BATER *et al.*, 2024).

Figura 12 - Mapa da Estônia

Fonte: (BATER *et al.*, 2024)

A Estônia foi dominada por potências estrangeiras durante grande parte da sua história. No período de 1934 a 1940, a Estônia esteve sob um regime autoritário que representou uma derrocada em sua democracia. Os problemas em relação à independência da Estônia começaram a se formar em agosto de 1939, quando a Alemanha nazista e a União Soviética assinaram o Pacto de Não Agressão Nazi-Soviética (também conhecido como Pacto Molotov-Ribbentrop), dividindo Europa Oriental em esferas de influência. Movendo-se para capitalizar do seu lado do acordo, a União Soviética logo começou a pressionar Estônia, Letônia e Lituânia a assinarem o Pacto de Defesa e Assistência Mútua, que permitiria a Moscou posicionar 25.000 soldados na Estônia (ESTADOS UNIDOS, 1996, p. 18).

Nesta época o Presidente Päts enfrentava problemas de saúde e não tinha muito apoio externo, o que fez com que concordasse com a demanda soviética. Em junho de 1940, as forças soviéticas ocuparam completamente o país, alegando que a Estônia tinha "violado" os termos do tratado de assistência mútua. Com rápidas manobras políticas, o regime do líder soviético Joseph V. Stalin forçou então a instalação de um governo pró soviético e convocou novas eleições parlamentares em julho. O Partido Comunista da Estônia, que ressurgiu com menos de 150 membros, organizou uma lista única de candidatos. Enquanto isso Päts e outros líderes políticos da Estônia foram sorrateiramente deportados para a União Soviética ou assassinados (ESTADOS UNIDOS, 1996, p. 18).

Com o país ocupado e sob controle total da União Soviética, a eleição foi vencida pelos comunistas, com 92,8 por cento dos votos, o que na verdade representava uma eleição apenas de fachada. No dia 21 de julho de 1940 um novo parlamento declarou a Estônia uma república soviética e o pedido de adesão ao bloco comunista. Em Moscou, o Soviete Supremo atendeu ao pedido em 6 de agosto de 1940 (ESTADOS UNIDOS, 1996, p. 18).

A anexação da Estônia pela União Soviética foi interrompida em junho de 1941 após a invasão alemã. Ainda naquele ano sob domínio soviético marcas profundas foram deixadas aos estonianos. Além da aquisição de seus país e a rápida nacionalização da sua economia capitalista ocorrida em 13 a 14 de junho de 1941, os estonianos também viram a deportação em massa de cerca de 10.000 dos seus compatriotas para a Sibéria mesmo antes da invasão alemã. Dos apreendidos durante uma operação noturna, mais de 80 por cento eram mulheres, crianças ou pessoas idosas. O objetivo desta ação era causar pânico

na população e não neutralizar qualquer ameaça real ao regime. A ocupação alemã de 1941-44 intensificou mais ainda a repressão, especialmente da população judaica da Estônia, que contava com cerca de 2.000 judeus (ESTADOS UNIDOS, 1996, p. 19).

Em setembro de 1944, quando o Exército Vermelho novamente se aproximou da Estônia, as memórias do domínio soviético ressurgiram com bastante nitidez o que fez com que cerca de 70.000 estonianos fugissem do país para o exílio (ESTADOS UNIDOS, 1996, p. 19). A Estônia tinha sido forçada a se tornar parte da União Soviética quando o Exército Vermelho "libertou" a república báltica dos nazistas, durante o que os russos chamam de "A Grande Guerra Patriótica" (CLARKE; KNAKE, 2015).

Estes emigrados mais tarde formaram comunidades étnicas na Suécia, nos Estados Unidos, Canadá, Grã-Bretanha, Austrália entre outros lugares, e continuaram se manifestando pelos direitos da Estônia durante os próximos cinquenta anos. No total, de 1939 a 1945, a Estônia perdeu mais de 20 por cento da sua população devido à turbulência da União Soviética e da Alemanha (ESTADOS UNIDOS, 1996, p. 19).

Na campanha pela independência da URSS, a maioria dos estonianos desejava escapar e reverter o seu passado soviético após anos de um sufocante governo social e político; uma economia fraca e ineficaz; privação cultural sob uma política de "russificação[15]" e aumento do desperdício e destruição ambiental. Esse foi o sentimento que surgiu na "revolução do canto" de 1988, quando os estonianos se reuniram em grandes manifestações pacíficas para cantar suas canções nacionais e dar voz às suas frustrações reprimidas. Ao mesmo tempo, os estonianos estavam igualmente empenhados num futuro como uma nação independente desfrutando de prosperidade econômica numa Europa pós-Guerra Fria (ESTADOS UNIDOS, 1996, p. 11).

Em 1989, a cidade de Tallinn se tornou, mais uma vez, capital da Estônia independente, quando a União Soviética se desintegrou e muitas de suas repúblicas componentes se dissociaram de Moscou e da URSS. (CLARKE; KNAKE, 2015).

[15] A russificação deve ser compreendida mais amplamente do que uma simples predominância do russo como "cultura-rei" no aparato do Estado: ela significou também a etnicização da vida política da URSS, bastante visível para o mundo depois de sua desagregação em dezembro de 1991, quando os Estados Independentes definiram suas linhas de conflito sem alterar o contorno etno-federalizador da política das nacionalidades de Lênin (1870-1924) e Stálin (1879-1953) (VIANA, 2019, p.1).

Os defensores da independência obtiveram uma vitória clara nas eleições de março de 1990. Em 30 de março de 1990, a Assembleia Legislativa da Estônia declarou uma fase de transição para a independência. A independência foi declarada formalmente em agosto de 1991 e reconhecida pela União Soviética no mês seguinte (BATER *et al.*, 2024).

Em meados da década de 1990, a Estônia ainda tinha um legado do período soviético que não poderia ser facilmente esquecido ou posto de lado. Os desafios enfrentados pelos estonianos incluíram a integração de uma população russófona de 500.000 pessoas imigrada da era soviética, assim como o direcionamento de uma economia que se desenvolveu seguindo diretrizes impraticáveis ditadas por um cenário autoritário. O futuro, entretanto, não estava se desenrolando inteiramente como esperado para Estônia, Letônia e Lituânia. O alargamento do fosso entre os novos ricos e os novos pobres gerava pressão na coesão social dos estonianos. Na frente diplomática, um novo contexto europeu e uma real soberania da Estônia caminhavam a passos lentos para se materializar. A proximidade da Estônia com a vasta Rússia ainda era um fato, apesar de o desejo de se livrar da influência russa de uma vez por todas. A Europa pós-Guerra Fria calculou as suas políticas com um olhar atento para a superpotência a leste assim como nos dias quando a União Soviética ainda estava intacta (ESTADOS UNIDOS, 1996, p. 11–12).

Mesmo assim, após quatro anos de independência, completados em 1995, a pacificação interna do país e o ritmo de progresso se tornaram marcos na luta por uma independência verdadeira. Esses fatores ofereceram a melhor garantia para o avanço e progresso contínuo da nação (ESTADOS UNIDOS, 1996, p. 12).

> Em junho de 1992 foi adotada uma nova constituição e em setembro foram realizadas eleições legislativas e presidenciais, com Lennart Meri, apoiado pela aliança Isamaa (Pátria), eleito presidente. Entre as questões-chave para a Estônia independente estavam os direitos dos residentes da república que imigraram após a anexação soviética da Estônia em 1940. Estes estonianos não étnicos (na sua maioria russos étnicos) foram obrigados a solicitar a cidadania, com requisitos de naturalização incluindo proficiência na língua estoniana. As relações entre a Rússia e a Estônia foram tensas por causa desta questão e pela presença contínua na Estônia de tropas russas, que finalmente deixaram o país em agosto de 1994 (BATER *et al.*, 2024).

Depois de 50 anos de anexação à então União Soviética, a Estônia tratou de reconquistar a sua independência, mas o corte com laços com Moscou teve um preço a ser cobrado, a Estônia ficou sem uma estrutura central de governo e de abastecimento, cerca de 98% das relações comerciais eram com os soviéticos. O orçamento público no

primeiro ano após a independência era de 113 milhões de euros, ou seja, era menos de 100 euros por cidadão estoniano (STEFANO; JANKAVSKI; YOSHIDA, 2019, p.84).

Isso fez com o governo da Estônia se movesse para encontrar uma saída rápida para não correr o risco de ficar estagnado. Tratou de trabalhar a transição para uma economia de mercado, com reforma monetária, privatizações, abertura do comércio e uma lei que proibia déficits orçamentários. Além disso, tratou da necessidade de reorganizar um governo recém-nascido, de um viés ultrapassado e burocrático, atrelado aos tempos soviéticos para uma gestão pública digitalizada, um fenômeno que vem provocando mudanças profundas em alguns governos, conhecido como: digitalização (STEFANO; JANKAVSKI; YOSHIDA, 2019, p. 82 e 84).

Atualmente na Estônia, 99% dos serviços públicos são oferecidos digitalmente, apenas a oficialização do casamento ou do divórcio necessita ser feita pessoalmente. Além disso, 99% das transações bancárias são realizadas online e 98% dos negócios são abertos pela Internet, sendo que o processo dura apenas 18 minutos. Ou seja, toda essa digitalização do país classificou a Estônia pela OCDE (Organização para a Cooperação e Desenvolvimento Econômico), o clube dos países ricos, como uma das nações mais avançadas na transformação digital (STEFANO; JANKAVSKI; YOSHIDA, 2019, p.86).

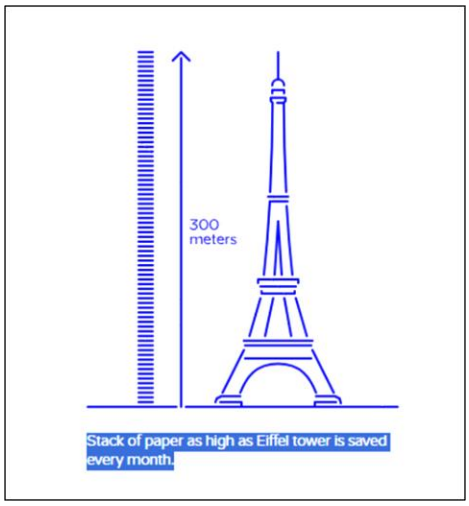
O cérebro por trás de todo esse desenvolvimento tecnológico é conhecido como plataforma X-Road, um software de código aberto e uma solução de ecossistema que fornece troca de dados unificados e seguros entre organizações dos setores público e privado, é a espinha dorsal da e-Estônia[16]. Invisível, mas crucial, permite que os vários sistemas de informação de serviços eletrônicos dos setores público e privado do país se liguem e funcionem em harmonia (e-ESTONIA, 2023). Pode se dizer que nada mais é que um grande banco de dados compartilhado por governo e empresas para armazenamento de informações de todos os cidadãos, tudo atrelado a identidade do cidadão. Por exemplo, um médico, ao avaliar um paciente, tem acesso a todos os tratamentos, doenças e remédios tomados por esse paciente ao longo da vida. Para mudança de endereço não existe a necessidade de alterar em diferentes sistemas, basta ser

[16] A e-Estonia é hoje o projeto mais ambicioso em matéria de política tecnológica, pois inclui todos os membros do governo e altera a vida quotidiana dos cidadãos. Os serviços normais com os quais o governo está envolvido – legislação, votação, educação, justiça, cuidados de saúde, bancos, impostos, policiamento, e assim por diante – foram ligados digitalmente através de uma plataforma, interligando a nação (HELLER, 2017).

feito apenas uma vez para que seja refletida em todos os demais programas (GOMES, 2023).

Atualmente, cerca de 52.000 organizações são usuárias indiretas dos serviços da plataforma X-Road, onde são realizadas 2,2 bilhões de transações por ano quanto ao uso de 3.000 serviços eletrônicos disponíveis (e-ESTONIA, 2023). Estima-se que a digitalização no país resulte em uma economia anual de 2% do Produto Interno Bruto (PIB). A assinatura digital tem sido amplamente utilizada desde 2002, o que possibilitou economizar o equivalente a uma semana de trabalho por ano por adulto em idade ativa. Isso é aproximadamente igual a uma pilha de papel da altura da Torre Eiffel de economia por mês (ESTONIA, 2023), vide figura 13.

Figura 13 – Economia de papel por meio do processo de digitalização da Estônia



Fonte: (ESTONIA, 2023)

A Estônia por ser um país digitalizado está desenvolvendo a inteligência artificial para os seus serviços. No setor público, algoritmos podem, por exemplo, identificar padrões de comportamento de contribuintes na evasão de impostos, tratamento médico para pacientes de maior risco, ou problemas em obras de infraestrutura, como pontes, viadutos, estradas etc. Por meio da análise da coleta desses dados, governos poderão ser preditivos nas demandas da população, em vez de serem reativos, como ocorre na maioria dos governos (STEFANO; JANKAVSKI; YOSHIDA, 2019, p. 86).

> Na Estônia, cidadãos já podem ir à Justiça para questionar pequenas causas contratuais perante um...computador. (...) só podem contar com inteligência artificial (IA) os julgamentos de casos com valor inferior a 7 mil euros. As duas partes em uma disputa fazem o upload no sistema de suas informações relevantes e o programa emite uma decisão. Mas uma parte inconformada pode recorrer a um juiz humano. Já existem no país 100 “robôs” exercendo essa função (MELO, 2023).

Outra tecnologia que tem tomado espaço nos governos é o uso do *block-chain* para fornecer a infraestrutura para a criação de *criptmoedas*, como a *bitcoin.* A sua utilidade está em proporcionar a segurança dos dados das pessoas e dos cidadãos na crescente demanda do setor público (STEFANO; JANKAVSKI; YOSHIDA, 2019, p.87).

Na última edição do ranking da Organização da Nações Unidas (ONU) sobre governos digitais (*e-Government Survey*), o Brasil apareceu na 49ª colocação, 6º país das Américas, atrás dos Estados Unidos (10ª posição), Canadá (32ª), Uruguai (35ª), Chile (36ª) e Argentina (41ª). O país avançou cinco posições de 2020 para 2022 na região, obtendo o maior crescimento. Em relação aos serviços oferecidos online, o país saiu da 21ª posição para 11ª. São Paulo ocupou a 17ª posição globalmente no ranking de serviços online locais. O resultado foi fruto de uma série de iniciativas do governo, como a plataforma Gov.br, responsável em fornecer acesso centralizado a diversos serviços públicos por meio de uma identificação digital única com senha (EY, 2023).

Todos esses benefícios da digitalização de um governo têm também os seus contratempos, principalmente no que tange às atividades de *hackers*[17] e cibercriminosos. Quanto mais digital uma nação se torna, mais os cidadãos dependem de tecnologia para a execução das suas atividades corriqueiras. Caso os possíveis ataques cibernéticos neutralizem o funcionamento da rede de dados e o seu tráfego, colocar-se-iam em risco todos os serviços prestados no país: bancário, comercial, jurídico, hospitalar, governamental, dentre muitos outros. Foi exatamente essa situação que a Estônia vivenciou no ano de 2007.

[17] Um hacker é um indivíduo que usa computador, rede ou outras habilidades para resolver um problema técnico. O termo também pode se referir a qualquer pessoa que use suas habilidades para obter acesso não autorizado a sistemas ou redes para cometer crimes. Um hacker pode, por exemplo, roubar informações para ferir pessoas por meio de roubo de identidade ou derrubar um sistema e, muitas vezes, mantê-lo como refém para cobrar um resgate. O termo hacker tem sido utilizado historicamente com duplo sentido, às vezes sendo usado como um termo de admiração por indivíduos que exibem um alto grau de habilidade e criatividade na abordagem de problemas técnicos. No entanto, o termo também é comumente aplicado a indivíduos que usam essa habilidade para fins ilegais ou antiéticos. Hacker foi usado pela primeira vez na década de 1960 para descrever um programador ou um indivíduo que, em um período de recursos de computador altamente restritos, poderia aumentar a eficiência do código de computador de uma maneira que removesse ou *hackeasse* o excesso de instruções de código de máquina de um programa. Ele evoluiu ao longo dos anos para se referir a alguém com uma compreensão avançada de computadores, redes, programação ou *hardware* (CHAI; ROSENCRANCE, 2021).

2.1.1 Ataque cibernético na Estônia (2007)

A guerra cibernética entre a Rússia e a Estônia começou em 2007, depois de uma proposta parlamentar para realocar uma estátua (comumente conhecida como "Estátua de Bronze", figura 14) em homenagem aos soldados soviéticos que morreram ao libertar a Estônia da Alemanha nazista. Russos étnicos, compreendendo quase um quarto da população (GREENE, 2010), viam o monumento como um símbolo pelo qual os direitos das minorias deveriam ser respeitados enquanto muitos estonianos nativos o viam como um símbolo da ocupação soviética (EHALA, 2009, p.13).

> O Exército Vermelho, ou pelo menos o Partido Comunista da União Soviética, não queria que os estonianos, ou qualquer outro povo do leste europeu, se esquecessem dos sacrifícios que foram feitos para "libertá-los". Assim, em Tallinn, como na maioria das capitais do leste europeu, eles ergueram uma dessas gigantes e heroicas estátuas de um soldado do Exército Vermelho, pelas quais os líderes soviéticos tinham tanto apreço. Muitas vezes, essas estátuas de bronze eram colocadas em cima dos túmulos de soldados do Exército Vermelho. (...) Parece que essas estátuas significam muito para os russos, assim como as sepulturas de soldados americanos mortos na Segunda Grande Guerra em países estrangeiros são consideradas solo sagrado para muitos veteranos americanos, suas famílias e seus descendentes. Tais estátuas também tiveram um significado importante para aqueles que foram "libertados", mas de forma completamente diferente. As estátuas e os cadáveres dos soldados do Exército Vermelho sob elas se tornaram, simbolicamente, um para-raios. Em Tallinn, a estátua também atraiu relâmpagos cibernéticos (CLARKE; KNAKE, 2015).

A situação ficou tensa em 9 de maio de 2006, quando dois membros da direita nacionalista estoniana foram à estátua durante as celebrações do Dia da Vitória[18] da União Soviética contra a Alemanha nazista. Eles carregaram a bandeira nacional da Estônia e uma faixa, enfatizando a ocupação soviética. Para evitar confrontos, a polícia removeu os dois ativistas. O evento foi transmitido pela mídia nacional. Esta humilhação criou uma forte reação emocional entre os estonianos e alguns políticos prometeram remover este símbolo de ocupação do centro de Tallinn. Enquanto a remoção do monumento tornou-se uma promessa de campanha eleitoral, a ideia, da mídia estoniana, de que a construção do monumento era o símbolo da ocupação soviética na Estônia, foi reforçada (EHALA, 2009, p. 13).

[18] O conflito, que durou quatro anos, gerou cerca de 45 milhões de mortes, entre eles, 27 milhões de soviéticos. Por isso, na Rússia, umas das 15 repúblicas socialistas soviéticas, anualmente celebra a memória dos mortos em combate e o legado da URSS na defesa da paz mundial com um desfile militar na Praça Vermelha de Moscou (MELLO, 2021).

Figura 14 – Homenagem ao Soldado Soviético na Segunda Guerra Mundial localizado na Estônia

Fonte: (EHALA, 2009, p.05)

Após a independência da Estônia ao final da Guerra Fria, a maioria dos estonianos reivindicavam que qualquer símbolo das cinco décadas de ocupação soviética fosse removido. Em fevereiro de 2007, o legislativo aprovou a Lei das Estruturas Proibidas indicando que qualquer coisa que denotasse a ocupação deveria ser derrubada, incluindo o soldado gigante de bronze (CLARKE; KNAKE, 2015).

> Na madrugada do dia 27 de abril de 2007, conhecida como Noite de Bronze, após uma reunião noturna da comissão de crise do país, o governo estônio removeu a estátua de bronze de 1,80 m de altura no centro de Tallinn, capital da Estônia. O monumento foi construído pelos soviéticos em 1947 para comemorar os mortos na guerra, depois de expulsarem os nazistas da região no final da Segunda Guerra Mundial. Para muitos cidadãos da Estônia, a estátua era um símbolo de uma ocupação opressiva, que lembrava a deportação de milhares de estonianos para a Sibéria. Após 16 anos de independência, os estônios reuniram coragem para ignorar os protestos do governo russo, que tinha avisado em tom ameaçador que a remoção seria desastrosa para a Estônia. (...) Mesmo antes da remoção, a violência eclodiu nas ruas de Tallinn. Os manifestantes quebraram vitrines de lojas, capotaram carros e atiraram pedras contra a tropa de choque. A maioria dos manifestantes eram de etnia russa, que representavam um quarto da população do país. Mas a luta cessou rapidamente; centenas de pessoas foram presas, as janelas foram reparadas e os varredores de rua limparam tudo na manhã de 28 de abril (DAVIS, 2007).

As autoridades rapidamente intervieram e moveram a estátua para uma nova localização protegida em um cemitério militar. Longe de aplacar a disputa, o movimento incendiou as respostas de nacionalistas indignadas na mídia de Moscou e na Duma Federal, o Legislativo da Federação Russa (CLARKE; KNAKE, 2015).

Por um lado, a Rússia agiu como sucessora da União Soviética e defensora da sua glória militar. O que incomodou o discurso oficial russo foi de ter sido questionado quanto ao papel libertador do Exército soviético em 1941-1945 e de ver a reabilitação da Alemanha nazista para as elites políticas dos três países bálticos (Estônia, Letônia e Lituânia). Sendo que a Estônia foi a mais censurada pela sua relutância em reconhecer a contribuição sacrificial da União Soviética na derrota da Alemanha nazista. Tais gestos, mesmo que simbólicos, em equiparar os papéis de Hitler e de Stalin ou desvalorizar a interpretação consensual sobre os resultados da II Guerra Mundial, foram recebidos com irritação por Moscou, e foram interpretados como a confirmação das alegadas transgressões da Estônia no plano dos princípios fundamentais da constituição do pós-II Guerra Mundial (MAKARYCHEV, 2009, p.56).

Foi então que o conflito se mudou dos protestos urbanos para o espaço cibernético, ou ciberespaço. Na primeira noite dos protestos, 27 de abril, fóruns de discussão, salas de bate-papo, blogs e redes sociais russas, ou seja, as mídias sociais foram inundadas com apelos para realizar uma ação contra a Estônia, a fim de atingir alvos da Internet. Esses sites forneciam ferramentas fáceis de usar e uma lista de alvos que os russos poderiam atacar. As postagens e ferramentas se tornaram populares, permitindo a participação de cidadãos sem conhecimento técnico em ataque cibernético. A lista inicial de alvos incluía o parlamento estoniano, a presidência e vários ministérios do governo. Isso deu início a uma Distribuição de Ataque de Negação de Serviço (DDoS), alimentando sites com tráfego, tornando-os inacessíveis. O sucesso dos ataques incentivou mais usuários a participar, enviando mais de 4 milhões de pacotes de dados por segundo para o país em contraste com o tráfego habitual da Estônia de 20.000 pacotes por segundo (ASHRAF, 2023, p.5559).

> Um ataque cibernético de negação de serviço é aquele que tenta impedir o uso legítimo de recursos de informática. Quando vários computadores são empregados para atingir esse objetivo, ele se torna um ataque distribuído de negação de serviço. Uma forma de categorizar esses ataques é fazendo a distinção entre os semânticos e os que empregam força bruta. A negação de serviço semântica tira proveito de uma característica ou de um defeito de software do sistema visado. Um ataque de força bruta (ou de "inundação") acontece quando o sistema visado recebe um volume de dados maior do que pode suportar, via Internet, o que esgota os recursos de comando e controle do servidor, tornando-o indisponível (SHAKARIAN, 2011, p.67)

Normalmente um DDoS é considerado um pequeno incômodo quando direcionado para um respectivo sítio da Internet, e não uma arma potente do arsenal

cibernético. No entanto, o ataque cibernético sofrido pela Estônia foi uma tempestade pré-programada de tráfego na Internet com o intuito de derrubar ou congestionar uma rede de dados. De uma hora para outra, os servidores que hospedavam as páginas mais utilizadas na Estônia foram inundados com pedidos de acesso. Foram tantas requisições que os sites não suportaram e entraram em colapso devido à sobrecarga de pedido e por isso deixaram de funcionar. Diversos outros *sites* ficaram tão sobrecarregados com a quantidade de *pings*[19] recebidos que ficaram totalmente inacessíveis por vários dias. Estonianos não podiam acessar seus bancos on-line, os sites de seus jornais ou os serviços eletrônicos do governo (CLARKE; KNAKE, 2015).

> O resultado para os cidadãos estônios foi que os caixas automáticos e os serviços bancários *online* ficaram esporadicamente fora de serviço; os funcionários do governo não conseguiam se comunicar por e-mail; e os jornais e as emissoras descobriram subitamente que não conseguiam transmitir as notícias (McGUINNESS, 2017).

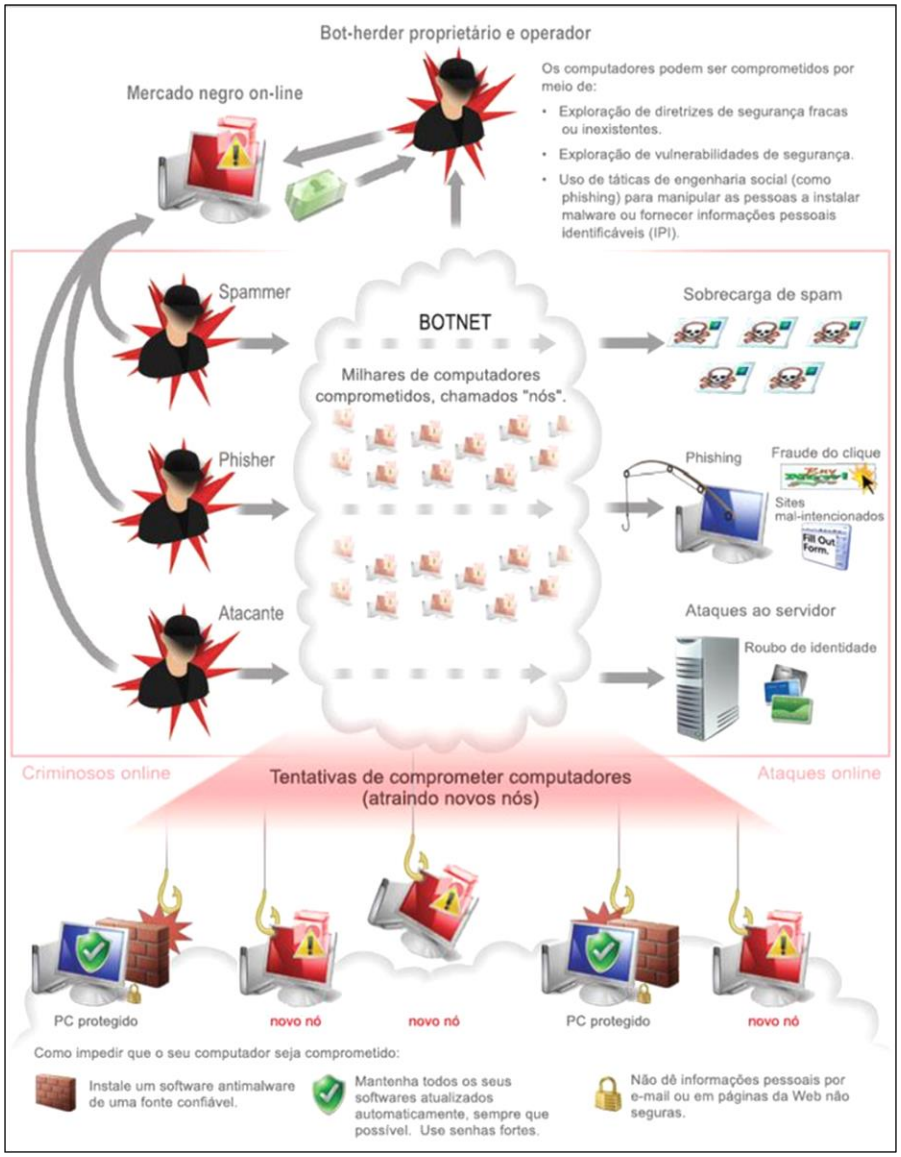
Enormes quantidades de *spams* foram enviadas por *botnets* e numerosa quantidade de solicitações *on-line* robotizadas inundaram os servidores de dados da Estônia. Um *botnet* se refere a um grupo de computadores infectado por malware e sob controle de um indivíduo mal-intencionado. O termo *botnet* é a combinação das palavras "*robot*" e "*network*" (robô e rede em inglês, respectivamente), e cada dispositivo infectado se chama *bot* (CLOUDFLARE, 2023).

O *bot* nada mais é que um programa de software que executa tarefas automatizadas, repetidas e pré-definidas (KASPERSKY, 2023a). Segundo a empresa de antivírus Symantec, os *bots* podem ser "bons" quando utilizados para a coleta de informações e interação automática com mensagens instantâneas. Os *bots* também podem

[19] Ping ou latência é um comando que serve para testar a conectividade entre equipamentos de uma rede utilizando o protocolo ICMP. A palavra "ping" é a abreviação do termo em inglês "*Packet Internet Network Grouper*", que significa algo como "Agrupador de Pacotes da Internet". Esse comando basicamente envia dados para esses equipamentos e fica aguardando respostas. Ele está disponível em praticamente todos os sistemas operacionais utilizados atualmente. O seu funcionamento envolve o envio de pacotes para o equipamento de destino e "fiscaliza" o tempo de resposta. Se o equipamento de destino estiver em funcionamento, a resposta, ou "pong" (referindo-se ao jogo ping-pong), é enviada para o computador que enviou o ping. Dessa forma, é possível saber se o tempo foi alto ou não. É importante ressaltar que, apesar da analogia com o jogo de ping-pong, segundo o autor da ferramenta, Mike Muuss, o objetivo ao dar o nome era fazer uma comparação com o som de um sonar (NASCIMENTO, 2014).

ser maliciosos quando têm habilidade de se auto propagar para coletar senhas, obter informações financeiras, lançar ataques de negação de serviço (DoS) (NORTON, 2018).

Figura 15 - Representação de uma *botnet*



Fonte: (MACEDO, 2013)

A representação de uma *botnet* demonstrada na figura 15, o *bot-herder* ou o proprietário e operador do ataque controla de forma remota os computadores atacantes ou computadores “zumbis”, representado na imagem pelos “nós”. Os zumbis atacam seguindo instruções que são acionadas sem o conhecimento de seus usuários. A atividade maliciosa ocorre em segundo plano, não sendo visível na tela do usuário.

> O que pode ter acontecido, muitas vezes semanas ou meses antes de uma *botnet* atacar, é que o usuário acessou inocentemente uma página onde, sem que tenha percebido “foi baixado” o software que transformou o seu computador em um zumbi. Ou então abriu um e-mail, talvez até mesmo de alguém conhecido, permitindo que o software zumbi fosse

> descarregado. Um antivírus atualizado e um firewall local podem bloquear essas infecções, mas os hackers estão constantemente descobrindo maneiras novas de contornar essas defesas(CLARKE; KNAKE, 2015).
>
> O firewall é um sistema de segurança de rede de computadores que limita o tráfego de entrada, saída ou trocas dentro de uma rede privada. Este *software* ou *hardware* funciona bloqueando seletivamente ou permitindo pacotes de dados. Em geral, destina-se a impedir que qualquer pessoa – dentro ou fora de uma rede privada – se envolva em atividades nocivas na web, ajudando a prevenir atividades mal-intencionadas ou que possam danificar o sistema. Os firewalls são como fronteiras bloqueadas ou cancelas que gerenciam a viagem de atividades permitidas ou proibidas na Internet em uma rede privada. Trocando em miúdos, os firewalls de segurança da rede destinam-se ao gerenciamento do tráfego da web – normalmente com o objetivo de desacelerar a disseminação de ameaças lá encontradas (KOVACS, 2021).

Segundo Liisa Past (McGUINNESS, 2017), especialista em defesa cibernética do Sistema de Informação da Estônia, a agressão cibernética é muito diferente da guerra cinética", explicou ela. "Ela permite criar confusão, ao mesmo tempo que permanece bem abaixo do nível de um ataque armado. Tais ataques não são específicos das tensões entre o Ocidente e a Rússia. Todas as sociedades modernas são vulneráveis". Isto significa que um país hostil pode criar perturbação e instabilidade num país da Organização do Tratado do Atlântico Norte (OTAN) como a Estônia, sem receio de retaliação militar por parte dos aliados da OTAN.

Por sua vez, a Estônia havia alegado que as máquinas de controle finais estavam fisicamente instaladas na Rússia, e que o código do programa havia sido escrito em alfabeto cirílico[20]. O governo russo indignou-se com o fato de que pudesse estar envolvido em uma guerra cibernética contra a Estônia. Mesmo existindo um acordo bilateral vigente para que houvesse cooperação para investigar o ataque cibernético, o governo russo recusou o pedido diplomático formal da Estônia de assistência para identificar os atacantes. Após terem sido comunicados que alguns dos endereços de IP dos ataques pertenciam a Rússia, alguns oficiais do governo admitiram ser possível que alguns russos nacionalistas estivessem envolvidos nos ataques, por uma sensação de indignação com o

[20] Por volta do ano 863, os irmãos Cirilo e Metódio, sob as ordens do Imperador Bizantino Miguel III, estruturaram o alfabeto para a língua eslava. A expansão do alfabeto cirílico está associada, principalmente, às atividades de uma escola búlgara (depois de Cirilo e Metódio). Na Bulgária, o rei São Boris, em 860, se converteu ao cristianismo e a Bulgária se transformou no centro de propagação da literatura eslava. Com isso foi criada a primeira Escola de Livro Eslava. A partir daí, eles começaram a reescrever os originais dos livros litúrgicos de Cirilo e a fazer as novas traduções eslavas da língua grega. Desse modo, surgem as primeiras obras originais em língua eslava antiga. Mais tarde, o idioma eslavo entra na Sérvia e, no final do século X, torna-se a língua oficial da Igreja na Rus Kievana. O alfabeto eslavônico (também chamado de velho-eslavo ou cirílico) foi composto principalmente por caracteres gregos, adicionando-se algumas letras hebraicas e árabes (MAZNOVA, 2010).

que a Estônia tinha feito, tratando assim de resolver o assunto com as próprias mãos (CLARKE; KNAKE, 2015).

Neste contexto, o artigo cinco da aliança dos países membros da OTAN, que garante que os membros se defendam, mesmo que o ataque seja no ciberespaço, não pode ser usado, pois só seria acionado se um ataque cibernético resultasse numa grande perda de vidas equivalente à ação militar tradicional. Identificar quem foi o responsável também dificultou a retaliação, pois não havia provas concretas de que estes ataques tenham sido realmente perpetrados pelo governo russo. Os ataques do Soldado de Bronze podem ser considerados os primeiros ataques cibernéticos suspeitos de uma ação estatal a outra nação (McGUINNESS, 2017).

Em agosto de 2022, a Estônia voltou a ser alvo de um novo ataque cibernético de grandes proporções. Um grupo de hackers, conhecido como *Killnet*[21], baseado na Rússia, reivindicou a responsabilidade pelo ataque em seu canal do *Telegram*. Diversos serviços digitais do governo da Estônia foram atacados, sistemas de pagamento, bancos, órgãos governamentais, serviços de saúde, educação, o que bloqueou o acesso a mais de 200 instituições públicas e privadas. Foram múltiplos ataques de *DDoS*, considerado o pior dos ataques cibernéticos já sofridos pela Estônia desde 2007. Acredita-se que o ataque ocorreu em resposta do governo estoniano ter removido um monumento de um tanque da era soviética, modelo T-34, na cidade de Narva (figura 16), uma região cuja população é predominantemente russófona (CISO, 2022).

[21] Killnet é um grupo de *hackers* pró-Rússia conhecido por seus ataques de negação de serviço direcionados a sites governamentais e de empresas privadas em países que apoiaram a Ucrânia durante a invasão russa da Ucrânia em 2022 (RADWARE, 2023).

Figura 16 - Tanque soviético T-34 na cidade de Narva

Fonte: (WHYTE, 2022)

De acordo com o governo de Tallin, o ataque foi 50 vezes mais intenso do que o anterior, com 40 milhões de solicitações de acesso. No entanto, o impacto do ataque foi limitado e passou "largamente despercebido". Apesar de a Estônia ser uma nação pequena, com uma população de 1,4 milhão de habitantes, possui uma forte infraestrutura de defesa cibernética que ocupa o quarto lugar do mundo, atrás dos Estados Unidos, Reino Unido e da Arábia Saudita; e o segundo lugar da Europa, conforme o Índice Global de Segurança Cibernética (GCI), ano de 2020 (GCI, 2020, p.25 e 30), atrás somente do Reino Unido.

2.2. Caso 2: Guerra da Geórgia e a Rússia (2008)

Este estudo de caso apresenta um contexto histórico em relação ao conflito bélico ocorrido entre as nações da Rússia e Geórgia, em agosto de 2008. Por último, trata da guerra cibernética a fim de demonstrar como ocorreu o ataque aos servidores de dados da Geórgia e como isso foi usado para uma posterior invasão do exército russo via aérea, terrestre e marítima.

2.2.1. Fim da URSS e a nova Rússia

A Rússia é um verdadeiro continente eurasiano (parte na Europa e parte na Ásia), que constituiu o império russo e depois a antiga União das Repúblicas Socialistas Soviéticas (URSS). Mesmo após a dissolução da URSS, a Federação da Rússia é ainda o país mais extenso do planeta. Compreende 11 fusos horários, desde o Estreito de Bering,

a Leste, até o limite com a Estônia, a Oeste, isto é, quase metade dos 24 fusos horários do globo terrestre (AGUIAR, 2002, p. 203 - 204).

Considerado o maior país do mundo com uma área total de 17.125.178 metros quadrados. Faz fronteira com 18 países (é o recorde mundial de quantidade de estados e de extensão da fronteira) - a Noruega, a Finlândia, a Estônia, a Letônia, a Lituânia, a Bielorrússia, a Polônia, a Ucrânia, a Geórgia, o Azerbaijão, a Abkházia, a Ossétia do Sul, o Cazaquistão, a China, a Mongólia, a Coreia do Norte, o Japão e os Estados Unidos da América (RÚSSIA, 2023). A figura 17 faz uma comparação entre a área da Rússia atual com a área dos Estados Unidos.

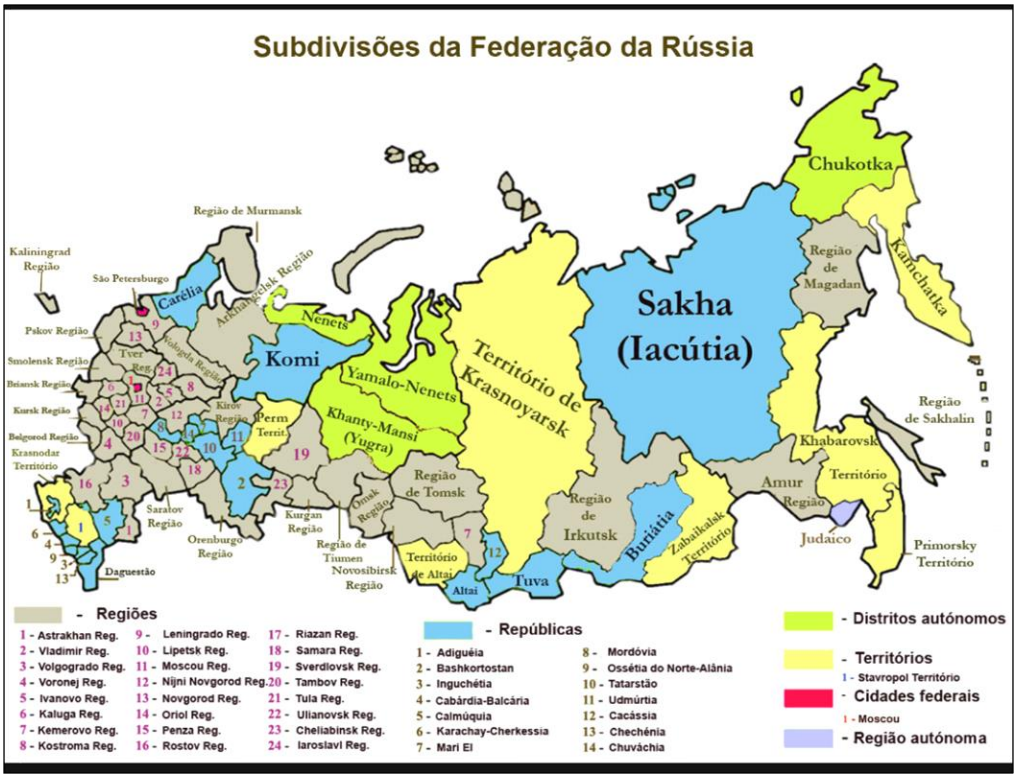
Figura 17 - Área da Rússia em comparação aos EUA

Fonte: (CIA.gov, 2023)

A Rússia possui características geográficas únicas; é um dos países mais ricos do mundo em recursos naturais e minerais. Sua população é de 146 milhões de pessoas, é a nona maior do mundo, é um estado multinacional em que moram os representantes de 176 nações e nacionalidades que professam diferentes religiões e falam mais de cem idiomas (RÚSSIA, 2023). Ela é constituída por 83 subdivisões administrativas (vide figura 18): 21 repúblicas, 9 territórios ou *krais*, 46 regiões ou *oblasts* (províncias – regiões autônomas administradas por um governador), 1 região autônoma (*oblast* autônoma

judaica)[22], 4 distritos autónomos e 2 cidades autônomas ou federais (Moscou e São Petersburgo) (RUSSOBRAS, 2023).

Figura 18 - Subdivisões da Federação da Rússia



Fonte: (RUSSOBRAS, 2023a)

Após a Revolução Russa de 1917 foi formada a União das Repúblicas Socialistas Soviéticas (URSS), constituída em 1922, cuja existência tornou-se um dos elementos estruturantes decisivos do quadro político e social estabelecido por quase todo o século XX (RODRIGUES, 2006, p.13). O Estado Soviético original foi ideologicamente concebido como temporário, provisório, transitório entre a era do capitalismo, nacionalismo e imperialismo, estabelecida para ser um exemplo de relações justas, não exploradoras, um modelo de integração de países (SUNY, 2008, p.86).

[22] Em 1930, foi criado o Distrito Nacional Judaico, como entidade nacional e territorial, para cá foram reassentados os judeus de toda a União Soviética. Em 7 de Maio de 1934 o Distrito Nacional Judaico foi transformado em Região Autônoma Judaica. No entanto, apesar do nome, os judeus nunca constituíram a maioria da população da região. E depois da imigração em massa para Israel em 1970-1990, na Região Autônoma Judaica os judeus são só um pouco mais de 1% da população. Mas o nome e o status da região autônoma, apoiados por um único toque simbólico e cultural e o destino histórico foram preservados (RUSSOBRAS, 2023b).

A radical transformação da paisagem soviética permitiu que milhões de pessoas melhorassem seu nível de vida e que outros milhões mergulhassem na degradação. No fim dos anos 30, os resultados da industrialização acelerada eram visíveis. Era o começo da disseminação de um dos mais vigorosos mitos políticos modernos: a construção de um mundo novo, diferente de tudo que a humanidade conheceu. Por mais parcial que fosse a narrativa de uma utopia soviética, ela exprimia uma percepção racionalizada do presente e do futuro da coletividade (FERREIRA, 1998, p.06).

Em 1985, um reformador apaixonado, Mikhail Gorbachev, chegou ao poder como secretário-geral do Partido Comunista soviético. Aos 54 anos, iniciou uma série de reformas para dar um novo fôlego ao país, que estava estagnado. Gorbachev lançou sua campanha para transformar o socialismo soviético com os slogans *Perestroika*, ou reconstrução e reestruturação (da estrutura econômica e política), e *Glasnost*, ou abertura e liberdade de informação e de expressão (HOBSBAWM, 1995).

A política da *Perestroika* de Gorbachev introduziu alguns princípios de mercado, mas a gigantesca economia soviética era pesada demais para ser reformada rapidamente. A política de *Glasnost* de Gorbachev visava a permitir maior liberdade de expressão em um país que passou décadas sob um regime opressor em que as pessoas tinham muito medo de dizer o que pensavam, fazer perguntas ou reclamar. Gorbachev começou a abrir arquivos históricos que mostravam a verdadeira escala da repressão sob Joseph Stalin (líder soviético entre 1924 e 1953), que resultou na morte de milhões de pessoas. Ele encorajou um debate sobre o futuro da União Soviética e suas estruturas de poder, sobre como elas deveriam ser reformadas para seguir em frente (KHINKULOVA; IVSHINA, 2022).

A repulsa à cada vez mais monumental e generalizada corrupção da *Nomenklatura*[23] foi o combustível inicial para o processo de reforma, e Gorbachev teve apoio bastante sólido dos quadros econômicos à *Perestroika,* sobretudo dos pertencentes ao complexo industrial-militar, que queriam verdadeiramente melhorar a administração de uma economia estagnante e, em termos científicos e técnicos, paralítica (HOBSBAWM, 1995).

[23] Em tempos atuais, “nomenclatura” refere-se a um conjunto de termos peculiares a uma arte ou ciência. Quando, no entanto, aparece com “k”, como no original russo, o que predomina é o seu sentido político, herdado da Revolução Russa, que logo remete a privilégios. Durante todas as décadas que durou a União Soviética, membros do Partido Comunista ganhavam apartamentos luxuosos para morar, recebiam atendimento médico em clínicas especializadas, inacessíveis ao cidadão comum, punham seus filhos com mais facilidade em universidades e conseguiam alimentos e roupas a preços mais baixos (CAMPOS, 2017).

Segundo Daraktchiev (2013), o mecanismo dos danos causados pela *Nomenklatura* foi bastante simples:

1) ele se espalhou como o câncer e cresceu descontroladamente, consumindo assim parte cada vez maior do PIB do país;

2) inevitavelmente se envolveu em esquemas de corrupção a começar pelo "segmento de seu mercado" oficializado chamado "*lobby*"; passando por inúmeros e elaborados esquemas para desviar dinheiro das obras públicas;

3) desperdiçou prontamente dinheiro de sua nação para fins ideológicos: para participar de esforços de guerra; para exibição, ou de outra forma como parte da ideologia de exportação, como "assistência" às nações pobres, "ajuda humanitária", etc., independentemente do fato, os benfeitores em geral estavam em melhor situação do que muitos dos seus próprios compatriotas;

4) em termos intangíveis, causou imensos danos a longo prazo em sua causa nacional.

A desintegração econômica ajudou a adiantar a desintegração política, e foi por ela alimentada. Com o fim do Plano e das ordens do partido vindas do centro, não havia economia nacional efetiva, mas uma corrida, empreendida por qualquer comunidade, território ou outra unidade que pudesse consegui-lo, para a autoproteção e autossuficiência, ou trocas bilaterais (HOBSBAWM, 1995).

Os conservadores lançaram um golpe de Estado fracassado em agosto de 1991 para tentar remover Gorbachev do poder. Em vez de salvar a URSS, a tentativa malfadada precipitou seu fim. Menos de três dias depois, os líderes do golpe tentaram fugir do país, e Gorbachev voltou ao poder, mas por um breve período (KHINKULOVA; IVSHINA, 2022).

Boris Iéltsin assumiu a posição de líder político soviético e em dezembro de 1991 em reunião realizada em Minsk, os governantes da Rússia, Boris Iéltsin, da Bielorrússia, Stanislav Shusshkevitch e da Ucrânia, Leonid Kravtchuk selaram um acordo no qual declaravam a URSS e seu Estado extintos e anunciavam a criação de uma nova Comunidade de Estados Independentes, CEI (RODRIGUES, 2006, p. 267 - 268), formada por 11 das 15 nações até então soviéticas (NETTO, 2011), com exceção dos países bálticos e da Geórgia. A URSS foi extinta oficialmente no dia 31 de dezembro de 1991, com a Rússia herdando o Exército vermelho, o arsenal nuclear e a cadeira da União no Conselho de Segurança da Organização das Nações Unidas (PINTO, 2017).

A Comunidade de Estados Independentes conseguiu desempenhar um papel importante nos anos imediatos, uma vez que atenuou as ruturas e a instabilidade que se seguiram ao colapso da URSS, mas nunca se firmou como uma verdadeira aliança entre repúblicas e não evitou a hegemonia da Rússia, que se acentuou progressivamente e que é hoje uma evidência na geopolítica internacional (PINTO, 2017), conforme demonstrado na figura 19:

> Em 1991, com o fim da URSS, o bloco se desmembrou em Armênia, Azerbaijão, Bielorrússia, Estônia, Geórgia, Cazaquistão, Quirguistão, Letônia, Lituânia, Moldávia, Rússia, Tadjiquistão, Turcomenistão, Ucrânia e Uzbequistão. Mas alguns desses novos países sofrem até hoje com a sombra do extinto bloco socialista, o que influencia nas relações com o Ocidente.
> Em países como Letônia, Lituânia e Estônia, cidadãos russos perderam direitos políticos. A presença dos russos passou a ser vista como um legado da antiga União Soviética. Foram aprovadas leis para proibir o direito dos russos de ter a cidadania desses países. Até hoje, na Letônia e na Estônia, os russos têm uma cidadania limitada e não podem votar para presidente" (UFMG, 2017).

Figura 19 - URSS x Rússia atual

Fonte: (NETTO, 2011)

Não se pode atribuir apenas ao retrocesso econômico e político à derrota da URSS na disputa da Guerra Fria com os Estados Unidos. Acredita-se que um dos motivos tenha sido também o atraso tecnológico da União Soviética enfrentado na década de 80. De acordo com Vladimir Visotski (*apud* MILHAZES, 2009), após o fim da URSS, o que se

constatou foi uma “fuga de cérebros” para países estrangeiros, milhares de cientistas russos emigraram de seu país em busca de melhores condições de vida e de trabalho. Além disso, faltou investimento pelas autoridades no campo da pesquisa científica e tecnológica, na renovação do parque tecnológico, somando-se à degradação do nível de ensino do país.

> Constatada a situação de crise no início da década de 80, impõe-se explicar as razões da desaceleração da economia soviética. Em seu informe perante a sessão plenária do CC do PCUS de 11 de junho de 1985, Gorbatchev denunciou o que se seriam as principais mazelas da economia soviética: atraso tecnológico; desperdício crescente de matérias-primas e energia; baixa qualidade de muitos produtos industriais, que acarretava sua baixa competitividade no mercado mundial; baixo rendimento dos investimentos, excessivos e em grande parte efetuados em obras inacabadas e uma planificação desequilibrada e crescentemente desarticulada (MANDEL, 1989, p. 25, *apud* RODRIGUES, 2006, p.164).

Rodrigues (2006, p. 178) questiona o porquê de uma defasagem tecnológica tão grande em tão pouco tempo da URSS em relação aos países do Ocidente e do Japão. E quais seriam os fatores que poderiam explicar o atraso tecnológico. Parte da resposta vem do entendimento que a União Soviética tinha sim certas dificuldades de natureza técnica, como sistema de telefônico e de telecomunicações obsoletos, necessidade de especialistas em desenvolvimento de software, entre outros fatores. No entanto, esse atraso não se localizava no baixo nível de qualificação dos profissionais, engenheiros, cientistas e técnicos soviéticos, ou seja, a outra parte da resposta pode ser encontrada em fatores políticos e institucionais, no seguimento do regime e do sistema de gestão dos governantes soviéticos.

Para Rodrigues (2006, p. 179), o problema não era de ordem técnica que seria o impeditivo para a URSS não ter seguido o mesmo caminho trilhado pelo Japão depois da Segunda Guerra quanto ao desenvolvimento da tecnologia microeletrônica e computacional. O avanço tecnológico soviético nos anos 60 era evidente e concorria em termos de igualdade com os Estados Unidos, pois desenvolveu a tecnologia da bomba nuclear em pouco tempo depois do Ocidente. E não se constrói bombas nucleares e mísseis intercontinentais teleguiados, que acertam alvos com precisão a milhares de quilômetros de distância sem tecnologia de propulsão e orientação de voo altamente apurada, sem um domínio mínimo da tecnologia de comunicações por códigos.

A URSS na verdade estava à frente do Japão e da maioria dos países capitalistas europeus em diversas áreas, não haveria como conseguir isso se não tivesse avançado no campo científico e técnico. Outro exemplo foi o fato de ter saído na frente dos EUA na corrida espacial com seus foguetes, estação espacial e satélites. O desenvolvimento da

indústria aeronáutica com aviões militares supersônicos de caça e bombardeiros só eram igualadas ou superadas pelos norte-americanos. (RODRIGUES, 2006, p.178 - 179).

> Os avanços em ambos os setores, espacial e aeronáutico, supõem, por sua vez, relativo progresso técnico em diversas áreas como eletrônica, telecomunicações, propulsão e servomecanismos. Nada disso podia ser feito sem uma ampla e sólida base educacional, científica, tecnológica e profissional. Na verdade, não havia atraso científico e tecnológico pronunciado da URSS até pelo menos o início dos anos 70, com exceção de algumas áreas, como a biotecnologia e a agricultura. Apesar de que seu parque industrial e tecnológico e sua infraestrutura estavam ficando rapidamente defasados e obsoletos – principalmente pela velocidade com que a tecnologia e a indústria capitalista se moviam para frente – durante a década de 70 não se podia falar em atraso significativo da URSS no domínio da pesquisa científica pura em relação aos Estados Unidos, Japão e Europa. Os físicos e matemáticos soviéticos destacavam-se entre os melhores do mundo. Os livros de cálculo integral e diferencial russos, por exemplo, eram referências, sendo utilizados em cursos de ciências exatas em todo o mundo (RODRIGUES, 2006, p.179).

A argumentação apresentada por Milhazes referente à defasagem tecnológica dos soviéticos em relação ao baixo nível cultural, educacional e de qualificação técnica dos profissionais, como a falta de pesquisa e de desenvolvimento técnico e científico, bem como a fuga de cientistas para outros países, poderiam até terem contribuído para o fracasso da URSS. Porém outros fatores seriam determinantes para o fim da União Soviética no início da década de 90. Para Rodrigues (2006, p.182 – 183) o desenvolvimento da ciência e da tecnologia soviéticas, nas décadas finais da URSS, ficou estagnado em razão da gestão burocrática e pelo controle ideológico e pela repressão política. As novas descobertas dos órgãos de pesquisa soviéticos terminavam por ter sua utilização restrita para fins específicos, geralmente militares, sem poder disseminar-se pelo conjunto do mecanismo econômico. Entende-se que um ambiente democrático é mais propício para o desenvolvimento do progresso social e tecnológico, do que um regime político ditatorial, cuja crítica ao funcionamento estatal seria tratada como um crime contra o Estado, cerceando e inibindo a construção de um espaço propício à criatividade e à inovação.

Após o fim da Guerra Fria, a Rússia tem ampliado a sua inserção no espaço cibernético e o seu desenvolvimento na área de tecnologia da informação. Em razão de diversas disputas territoriais e da luta por influência política em países da antiga URSS, a Rússia tem sido acusada de autoria de diversos ataques cibernéticos a países fronteiriços, o que tem gerado transtornos nos serviços telemáticos desses países. A exemplo do que ocorreu com a Estônia em 2007 e com a guerra entre a Rússia e a Georgia no ano de 2008.

2.2.2. Breve história sobre a Geórgia

Geórgia é um país da Transcaucásia localizado no extremo leste do Mar Negro e ao sul das montanhas do Grande Cáucaso. É limitado ao norte e nordeste pela Rússia, a leste e sudeste pelo Azerbaijão, ao sul pela Armênia e pela Turquia e a oeste pelo Mar Negro. A Geórgia inclui três enclaves étnicos: Abecásia, no Noroeste; Ajaria, no Sudoeste; e Ossétia do Sul, no Norte. A capital da Geórgia é Tbilisi.

Figura 20 – Mapa político da Geórgia, Abecásia e Ossétia do Sul

Fonte: (MUNDO, 2024)

Possui um território de 69.700 quilômetros quadrados. Atualmente, a população é de cerca de 3.713.800 milhões, segundo o censo de 2014, do Escritório de Estatística Nacional da Geórgia, conforme demonstrado na tabela 1.

Tabela 1 - Número da População da Estônia

მოსახლეობის რიცხოვნობა მოსახლეობის აღწერის შედეგებით (ათასი)
Number of population according to the population census data (thousands)

წელი Year	სულ Total	დასახლების ტიპი Type of settlement		სქესი Sex		ძირითადი ასაკობრივი ჯგუფები Major age groups		
		საქალაქო Urban	სასოფლო Rural	კაცი Males	ქალი Females	0-14	15-64	65+
1897	2 109.3	322.3	1 787.0	1 125.0	984.3	853.9	1 170.5	84.9
1926	2 666.5	594.2	2 072.3	1 347.5	1 319.0	1 032.1	1 490.8	143.6
1939	3 540.0	1 066.2	2 473.8	1 765.0	1 775.0	1 308.0	2 027.8	204.2
1959	4 044.0	1 712.9	2 331.1	1 865.3	2 178.7	1 184.6	2 549.5	309.9
1970	4 674.6	2 211.0	2 463.6	2 195.5	2 479.1	1 431.8	2 857.2	385.6
1979	4 993.2	2 548.7	2 444.5	2 338.9	2 654.3	1 297.6	3 233.9	461.7
1989	5 400.8	2 991.3	2 409.5	2 562.0	2 838.8	1 338.4	3 584.4	478.0
2002[1]	3 991.3	2 247.1	1 744.2	1 898.5	2 092.8	821.6	2 641.0	528.7
2014	3 713.8	2 122.6	1 591.2	1 772.8	1 941.0	691.3	2 492.3	530.2
				%				
1897	100.0	15.3	84.7	53.3	46.7	40.5	55.5	4.0
1926	100.0	22.3	77.7	50.5	49.5	38.7	55.9	5.4
1939	100.0	30.1	69.9	49.9	50.1	36.9	57.3	5.8
1959	100.0	42.4	57.6	46.1	53.9	29.3	63.0	7.7
1970	100.0	47.3	52.7	47.0	53.0	30.6	61.1	8.2
1979	100.0	51.0	49.0	46.8	53.2	26.0	64.8	9.2
1989	100.0	55.4	44.6	47.4	52.6	24.8	66.4	8.9
2002	100.0	56.3	43.7	47.6	52.4	20.6	66.2	13.2
2014	100.0	57.2	42.8	47.7	52.3	18.6	67.1	14.3

Fonte: (GEORGIA, 2023, p.11)

As raízes do povo georgiano estendem-se profundamente na história; sua herança cultural é igualmente antiga e rica. Durante o período medieval existiu um poderoso reino georgiano, atingindo seu apogeu entre os séculos X e XIII. Após um longo período de dominação turca e persa, a Geórgia foi anexada pelo império russo no século XIX. Um estado georgiano independente existiu de 1918 a 1921, quando foi incorporado à União Soviética. Em 1936, a Geórgia tornou-se uma república e continuou como tal até o colapso da União Soviética. Durante o período soviético, a economia georgiana foi modernizada e diversificada. Uma das repúblicas mais independentes da antiga URSS, a Geórgia declarou soberania em 19 de novembro de 1989 e independência em 9 de abril de 1991 (SUNY; DJIBLADZE; LANG, 2023).

A Geórgia e a Rússia tiveram diversos conflitos ao longo do tempo, desde a época dos czares. Em 1990, Geórgia entrou em conflito com a Ossétia do Sul e a Abecásia, que se prolongou até 1992. O fim de conflito só ocorreu quando a Rússia negociou com a Ossétia do Sul e a Geórgia a criação de uma força de paz.

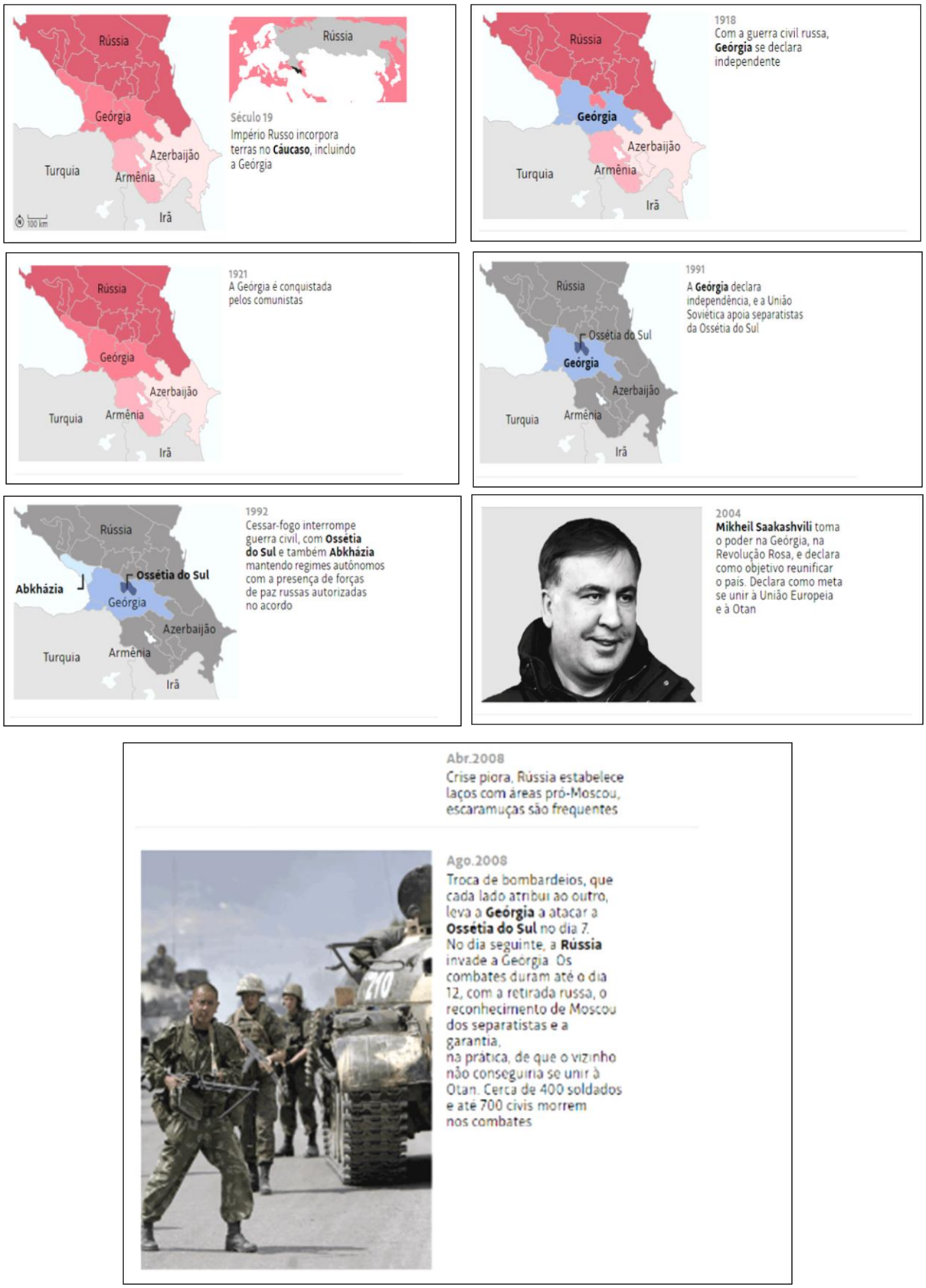
> Quando sete décadas mais tarde ocorreu o colapso da União Soviética e a Geórgia declarou sua independência, também os abecásios e sul-ossetas reivindicaram soberania sobre suas regiões. A recusa do governo central da Geórgia a reconhecer as independências levou à deflagração de intensos conflitos em ambas as regiões, cujos governos autoproclamados solicitaram apoio de Moscou.
> A intermediação russa congelou a situação: tropas de paz foram enviadas às duas regiões e lá se encontram até hoje; apesar de possuírem governos e instituições próprias, a Ossétia do Sul e a Abecásia jamais lograram ser reconhecidas como estados independentes pela comunidade internacional (RANDIG, 2008).

Em 2004, Mikheil Saakashvili assumiu a presidência da Geórgia, o que fez com que acirrasse a situação das repúblicas separatistas: Ossétia do Sul e Abecásia. Ele assumiu o governo com o compromisso de reconstituir a integridade territorial da Geórgia, o que implicava retomar o controle das regiões separatistas e buscou também a aproximação com os Estados Unidos, a União Europeia e a OTAN, desagradando os interesses de Moscou, que via o país vizinho como parte importante de sua esfera de influência (RANDIG, 2008).

> Mikheil Saakashvili, que presidiu a Georgia entre 2004 e 2013, foi preso em 2021 após julgamento à revelia. Líder da oposição, ele fazia greve de fome havia 50 dias para protestar contra a prisão. Segundo um boletim médico divulgado no dia 05/12/2022 por seus advogados, o ex-presidente da Geórgia, Mikheil Saakashvili, foi envenenado na prisão com metais pesados e corre o risco de morrer se não receber o tratamento adequado. Em um relatório divulgado pela equipe jurídica de Saakashvili, o toxicologista David Smith escreveu que "exames revelaram a presença de metais pesados" no corpo do ex-político, e que seus sintomas se devem a "envenenamento por metais pesados"(PRESSE, 2022). O Parlamento Europeu por meio de Resolução, de 15 de fevereiro de 2023, sobre a situação do antigo Presidente da Geórgia, Mikheil Saakashvili (2023/2543 - RSP) manifestou viva preocupação com a deterioração do estado de saúde do antigo Presidente Mikheil Saakashvili e com a resposta inadequada das autoridades georgianas até ao momento presente; considerou que o tratamento dos prisioneiros, como o antigo Presidente Mikheil Saakashvili, é um teste decisivo para o empenho do governo da Geórgia em relação aos valores europeus e para as suas aspirações europeias declaradas, incluindo o estatuto de país candidato (EUROPEU, 2023).

Com o passar do tempo, o quadro regional para Tbilisi, ao invés de melhorar o relacionamento diplomático com Moscou, degradou-se bastante: em abril de 2008, o Kremlin aproximou mais das duas áreas secessionistas com efeitos deletérios para a administração de Saakashvili (ARRAES; NOGUEIRA, 2020, p.08). Uma cronologia dos principais conflitos entre a Geórgia e a Rússia é demonstrado na figura 21.

Figura 21 - Geórgia e Rússia têm relação conflituosa desde os tempos dos czares



Fonte: (GIELOW, 2018)

2.2.3. O conflito bélico na Geórgia

No dia primeiro de agosto de 2008, rebeldes da Ossétia do Sul (ou agentes russos[24], a depender da versão que for contada) provocaram um conflito com a Geórgia organizando uma série de ataques de mísseis contra aldeias georgianas (CLARKE; KNAKE, 2015). Os bombardeamentos dos separatistas ossetos contra aldeias georgianas atraíram uma resposta esporádica das forças de manutenção da paz georgianas e de outros combatentes já na região (WHITMORE, 2008).

Na madrugada do dia 7 para o dia 8 de agosto, a Georgia utilizou do direito internacional para perpetrar o uso da força militar a fim de repelir os ataques de milícias da Ossétia do Sul às vilas georgianas e reconquistar a região separatista. A resposta militar segundo o governo da Geórgia tinha como motivo também impedir uma invasão russa que já se encontravam de prontidão quando o conflito iniciou. De qualquer forma, a decisão precipitada da Geórgia de submeter a Ossétia do Sul perturbou um *status quo* que, embora confuso e imperfeito, permitiu algum grau de estabilidade na região durante mais de uma década. A Rússia justificou o seu ataque às tropas da Geórgia com o uso de tropas do exército russo, ataques aéreos e forças navais como uma forma de impedir uma "genocídio" contra os ossetos e cidadãos russos que viviam na região da Ossétia do Sul (KING, 2009).

> O que talvez não tenha sido previsto por Saakashvili foi a reação russa. No dia seguinte, ataques aéreos começaram e 70 mil homens mobilizados para um exercício militar no norte do Cáucaso entraram em ação com outros 9.000 soldados separatistas. Navios russos no mar Negro foram acionados e, ao fim do conflito, soldados de Moscou já ocupavam território georgiano fora das duas áreas separatistas. Os cerca de 25 mil homens de Saakashvili estavam perdidos (GIELOW, 2018)

De acordo com Kakachia (2008, p.34) existiam indicadores preocupantes de preparação do conflito por parte de Moscou, sobretudo depois do reforço de tropas russas acima do quantitativo comum, como de múltiplas violações do espaço aéreo georgiano por caças russos, da derrubada de drones georgianos, além de um exercício militar em

[24] The New York Times relatou que o presidente da Geórgia, Mikheil Saakashvili, caíra na armadilha de Moscou e atraíra os russos de maneira trágica ao enviar seu exército à Ossétia do Sul. Ainda segundo o NYT, Vladimir Putin estaria por trás da agressão russa, e parecia determinado a retomar através da força e intimidação a maior parte possível da antiga União Soviética sem sofrer retaliações (The New York Times, 2008). No mesmo dia, outros periódicos reproduziram as acusações a Putin, armando que o então Primeiro-Ministro teria por hábito a utilização de manobras dissimuladas aprendidas nos manuais da KGB. No dia 02 de setembro, o Washington Post responsabilizou pelo conflito o "presidente transformado em primeiro ministro", Vladimir Putin, indicando que as tendências autoritárias na Rússia a tornariam cada vez mais agressiva contra democracias vizinhas (The Washington Post, 2008). O que chama a atenção é a total responsabilização da Rússia pelo conflito e a semelhança da identidade usualmente atribuída à antiga URSS durante a Guerra Fria à Rússia atual (MIELNICZUK, 2013, p.158).

larga escala perto da fronteira, que simulava a invasão da Geórgia. Esses exercícios sugeriam a possibilidade de uma ação militar da Rússia na Geórgia, planejada com meses de antecedência, aguardando apenas o pretexto apropriado para se concretizar.

De uma perspectiva estratégica global, a Guerra Russo-Georgiana pode também ser considerada uma operação de guerra psicológica. Acredita-se que o Presidente da Geórgia, Mikhail Saakashvili, foi provocado pela Rússia a desencadear este confronto militar desvantajoso. Na época a Secretária de Estado Norte Americano, Condoleezza Rice, alertou o Presidente Saakashvili para não cair na armadilha das provocações russas. Ela disse sobre ele: "Ele é orgulhoso e pode ser impulsivo, e todos nós nos preocupamos que ele poderia permitir que Moscou o provocasse a usar a força". É, portanto, possível, como se pensava Rice, que os bombardeamentos perpetrados pelos separatistas da Ossétia do Sul em aldeias na fronteira da Geórgia pretendiam provocar a ofensiva georgiana. Essa hipótese é reforçada pela alta prontidão e resposta rápida das forças russas, o que indica planejamento prévio avançado (CHIASSON, 2019, p.56).

Entende-se que o pretexto para o início do conflito partiu dos militares georgianos quando invadiram a Ossétia do Sul. Na verdade, essa provocação impulsionou a participação da Rússia em oposição à Geórgia repercutindo também na região de Abecásia (RANDIG, 2008). Após a vitória, a Rússia reconheceu ambas regiões separatistas como estados independentes, que por sua vez convidaram os russos a ficarem em seus respectivos territórios (CLARKE; KNAKE, 2015).

Há quem defenda que a ofensiva russa na região do Cáucaso seria uma volta às políticas da antiga União Soviética, o que poderia ser avaliada por uns como o possível retorno às práticas administrativas da finada União Soviética, ou seja, as da crença na manutenção territorial irrestrita ou mesmo da sua expansão sem amarras (ARRAES; NOGUEIRA, 2020, p.8). Embora o colapso do bloco socialista seja o pano de fundo do conflito, o renascimento do poder econômico, político e militar da Rússia, que havia saído da experiência comunista aniquilada, constitui a nova realidade da região (RAMINA, 2010, p. 3693).

> A guerra na Geórgia no verão de 2008 é um elemento central na análise deste debate. A Rússia aproveitou esta oportunidade para se afirmar no espaço pós-soviético perante a ingerência crescente ocidental e, acima de tudo, perante um conjunto de políticas e ações liderados pelos EUA, em particular, e considerados em Moscou como ultrapassando uma política de cooperação estratégica, com implicações diretas para a segurança da Rússia. O projeto do escudo de defesa antimíssil, o alargamento da Aliança Atlântica ao espaço

> CEI e a questão do Kosovo[25], por exemplo, demonstram o descontentamento russo. O pós -Geórgia revela o reposicionamento dos vários atores na área, onde a Rússia parece assumir um papel de destaque na sua afirmação enquanto ator fundamental no espaço CEI (FREIRE; SIMÃO, 2014, p.92).

Segundo Mielniczuk (2013, p. 165) as causas da guerra ente a Rússia e a Georgia poderiam ser atribuídas ao renascimento do nacionalismo georgiano e aos resultados do processo de crescimento das fronteiras da OTAN no leste Europeu. Acrescente-se o fato da independência de Kosovo, em fevereiro de 2008, sem a anuência de Moscou, o que se tornou um precedente para que uma possível intervenção russa resultasse na independência da Ossétia, mesmo que não tenha sido uma relação direta com o conflito no Cáucaso, a libertação de Kosovo do governo dos sérvios favoreceu de forma secundária para a assertividade da resposta russa e fortaleceu a tese de que as causas do conflito eram de responsabilidade do Ocidente, e não da Rússia. Causalidade que não minimiza o papel que a Rússia desempenhou para a realização do conflito. A pretensão dos russos era retomar, a partir de 2008, a categoria de potência emergente.

Para Macfarlane (2006, p.41 e 56) considera-se uma potência emergente quando são encontradas três caraterísticas: preponderância regional, aspirações ao protagonismo global e contestação da hegemonia norte-americana. O discurso de Macfarlane segue o entendimento que a Rússia ainda não é uma potência emergente no sentido convencional da expressão. Ou seja, a política externa russa é dominada pelo esforço para reverter o declínio substancial das décadas de 1980 e 1990 e estabelecer as bases internas para um retorno ao real (em oposição ao status simbólico) como uma grande potência. Isto implica a promoção de condições internacionais que permitam que esta nova configuração prossiga sem interferências externas. A outra grande prioridade na política externa é regional: restaurar influência russa sobre os antigos estados soviéticos - ou pelo menos para impedir a intrusão de potências externas nesse espaço, para limitar o crescimento de influências ocidentais e controlar tendências na região que possam produzir repercussões

[25] No caso da Ossétia do Sul, região pivô da Guerra do Cáucaso de 2008, não foi aplicada a mesma lógica do caso do Kosovo de 1999, quando as tropas da Organização do Tratado do Atlântico Norte – OTAN intervieram na região, e que posteriormente declarou sua independência da Sérvia em 17 de fevereiro de 2008. Se, ao contrário, as potências ocidentais seguissem as mesmas diretrizes deste último, deveriam aceitar a independência da Ossétia do Sul, de maioria russa, supostamente sufocada pela Geórgia. Nesse caso, talvez, a Rússia viesse a aceitar a independência de Kosovo, pois ambos os casos envolvem a modificação das fronteiras territoriais com bases étnicas, em aplicação do velho e revolucionário princípio francês das nacionalidades. Falta uniformidade no conteúdo e na aplicação do princípio da autodeterminação dos povos, para que o exercício discricionário do poder possa ser limitado por normas jurídicas, que por sua vez possam impedir o uso da violência, pela via da domesticação do poder pelo Direito (RAMINA, 2010, p.3692).

na própria Rússia. As relações da Rússia com potência hegemônica são complexas e parecem estar baseadas em uma compreensão realista da preponderância do poder norte-americano e também da hierarquia dos interesses políticos norte-americanos.

Quando Mikhail Saakashvili foi eleito presidente da Geórgia em 2004, assumiu o compromisso político de estreitar os laços com os Estados Unidos e a OTAN, como também unificar a regiões separatistas da Ossétia do Sul e Abecásia. Era tudo o que Moscou não queria, ou seja, mais um país da antiga União Soviética e vizinho de fronteira sob a influência do Ocidente, uma afronta e ameaça para os russos que desejavam alcançar novamente a posição de protagonista mundial.

Vladimir Putin como primeiro-ministro da Rússia em 2008 estabeleceu relações formais com as duas regiões separatistas, Ossétia do Sul e Abecásia, integradas economicamente ao país, apesar de serem consideradas pela ONU como parte da Geórgia. Putin, ao atacar e vencer os georgianos, teve como intenção deixar um "recado" que não toleraria mais ações ocidentais em seu "quintal".

2.2.4. O conflito cibernético na Geórgia

A invasão da Rússia na Ossétia do Sul e na Geórgia causou a morte de 1.100 pessoas no conflito, sendo que 400 só de civis e aproximadamente 200 mil perderam seus lares. De um ponto de vista maior, geopolítico, a vitória marcou o início da transformação de Vladimir Putin de um líder admirado por ter estabilizado o caos russo dos anos 1990 em uma espécie de vilão de seriado no Ocidente (GIELOW, 2018).

Antes que os combates começassem no mundo físico, ataques cibernéticos atingiram a rede de dados da Geórgia e prejudicaram a disponibilidade dos sítios (*sites,* em inglês) do governo da Geórgia. Nos estágios iniciais, foram realizados ataques de negação de serviço distribuído (*Distributed Denial of Service* - *DDoS*, em inglês) (CLARKE; KNAKE, 2015).

Esse tipo de ataque aproveita os limites de capacidade que se aplicam a todos os recursos de rede, como a infraestrutura que viabiliza o site de um governo (KASPERSKY, 2023b). No caso da Geórgia, os atacantes conduziram ataques *DDoS* básicos em sites do governo georgiano e invadiram o servidor web do site da presidência para realizar uma desfiguração da página da Internet, conhecido como *defacement* (em inglês), adicionando imagens que comparavam o líder georgiano, Mikheil Saakashvili, a Adolf Hitler (CLARKE; KNAKE, 2015).

> O *defacement* se refere a um ataque em que tanto a aparência, como o conteúdo de um site ou página da web é afetado, modificando, alterando e até excluindo o conteúdo originalmente disponibilizado, atacando sua disponibilidade e sua integridade. Isso significa, portanto, que o próprio código de construção da página afetada (HTML) está sendo alterado sem permissão. Porém, vale destacar que o *defacement* não se concentra apenas no código HTML, podendo atingir também outros componentes da página web (BRASIL, 2023c).

Segundo a matéria jornalística vinculada no site do Canal de Notícias G1, do dia 19/08/2008, teve como título o bombardeio virtual de *hackers* como o início ao ataque contra a Geórgia. Para os especialistas em conflitos, essa seria a primeira vez que a ação de atacar ciberneticamente um país coincidiria com uma guerra cinética, ou seja, uma guerra protagonizada por tanques, navios, aeronaves, soldados, etc.

> De acordo com especialistas técnicos em Internet, foi a primeira vez que um ataque virtual coincidiu com uma guerra real. Mas provavelmente não será a última, diz Bill Woodcock, diretor de pesquisa da *Packet Clearing House*, uma organização sem fins lucrativos que rastreia o tráfego da rede. Ele diz que cyber-ataques são tão baratos e fáceis de organizar, com poucas impressões digitais, que quase certamente permanecerão como marca dos combates modernos (G1, 2008).

Ainda de acordo com a reportagem, ataques de negação de serviço tiveram início em 2001 e desde então vêm sendo refinados em termos de força e sofisticação. O modo de operação é fazer uso de um grande quantitativo de computadores pessoais pirateados, tornando difícil ou impossível determinar quem está por trás de um ataque específico.

O ataque de DDoS perpetrado aos *web sites* da Geórgia foram captados no dia 19 de julho de 2008 por uma empresa de segurança da Internet. Três semanas depois, no dia 08 de agosto de 2008, especialistas em segurança observaram uma segunda rodada mais substancial de ataques *DDoS* contra sites da Geórgia. Os analistas observaram que esses ataques *DDoS* adicionais pareciam coincidir com o movimento das tropas russas para a Ossétia do Sul em resposta às operações militares georgianas lançadas no dia anterior na região. Em 10 de agosto, os ataques *DDoS* indisponibilizaram a maior parte da rede de dados governamental da Geórgia, diversos sites ficaram inoperantes (KORNS; KASTENBERG, 2008, p.60).

A passagem de ligação da Internet da Geórgia era conectada à Rússia e à Turquia. Em razão disso, a entrada da maioria dos roteadores da Rússia e da Turquia que enviava tráfego para a Geórgia foi inundada com os ataques a ponto que o tráfego de saída ficou incapaz de transmitir dados. Além disso, os atacantes assumiram o controle direto do resto dos roteadores que suportavam o tráfego para a Geórgia. Isso resultou na impossibilidade de os georgianos se conectarem a qualquer fonte de notícia ou informação externa, indisponibilizando o envio de e-mails para fora do país. A Geórgia efetivamente perdeu

o controle sobre o domínio ".ge" da nação e foi forçada a mudar muitos dos sites do seu governo para servidores de fora do país (CLARKE; KNAKE, 2015).

> O roteador é um aparelho usado em redes de computadores para o encaminhamento das informações acondicionadas em pacotes de dados, proporcionando conectividade entre os dispositivos como computadores, smartphones e tablets, em redes LAN com a Internet. Além disso, o roteador possui uma característica específica: buscar as melhores rotas para enviar e receber dados, podendo priorizar não só as transmissões mais curtas, como também as menos congestionadas (RIBEIRO, 2013).

> Os georgianos bem que tentaram defender seu ciberespaço utilizando "soluções alternativas" para frustrar os ataques DDoS, mas os russos rebateram cada movimento. A Geórgia tentou bloquear todo o tráfego vindo da Rússia. Os russos redirecionaram seus ataques para parecerem pacotes vindos da China. Além de um servidor mestre em Moscou para controlar todas as *botnets* usadas nos ataques, servidores no Canadá, Turquia e, ironicamente, na Estônia também foram utilizados. A Geórgia transferiu a página da Internet do presidente para um servidor no *Blogspot* do Google, localizado na Califórnia. Os russos então configuraram falsos sites presidenciais e direcionaram o tráfego para eles (CLARKE; KNAKE, 2015).

Certamente a campanha cibernética tinha como objetivo primário dar suporte a invasão da Rússia na Geórgia mirando na infraestrutura crítica do país. A escalada de ataques cibernéticos foi significativa segundo Handler (2012, p.224). Cinquenta e quatro websites da Geórgia foram atacados no total. Os alvos cibernéticos eram quase todos com a intenção de beneficiar os militares russos, o que incluía canais oficiais do governo georgiano, os meios de comunicação e setores da imprensa que, em se tratando de uma guerra convencional, seriam os primeiros lugares a serem atacados por mísseis e bombas na fase inicial dos combates.

Os setores bancários temendo danos internos aos seus sistemas, entenderam por bem que seria melhor desligar os seus servidores do que correrem o risco de os dados dos correntistas serem roubados e os seus sistemas invadidos. Com a indisponibilidade dos sistemas bancários, os russos voltaram a realizar *botnets* com objetivo de "congestionar" o tráfego dos bancos internacionais, simulando que os ataques cibernéticos estavam partindo da Geórgia. A resposta da maioria dos bancos estrangeiros foi a de encerrar suas conexões com o setor bancário georgiano. Sem acesso ao sistema de compensação do Ocidente, a Geórgia vivenciou a paralisação das operações bancárias internacionais. A mesma situação ocorreu com o sistema de cartão de créditos e da telefonia móvel (CLARKE; KNAKE, 2015).

> Nessa fase inicial, os ataques foram dirigidos principalmente contra sítios Internet do governo georgiano e da mídia local. As *botnets* russas empregaram negação de serviço por força bruta. As redes georgianas, devido à sua natureza débil, estavam mais

> suscetíveis a inundações do que as redes estonianas, que haviam sido atacadas pelos hackers russos no ano anterior. Na segunda fase, os sítios Internet da mídia e do governo georgianos continuaram a receber os ataques, mas a operação cibernética russa foi ampliada de modo a infligir danos a mais alvos, incluindo instituições financeiras, empresas, instituições de ensino, mídia ocidental (BBC e CNN) e um sítio Internet de hackers da Geórgia (SHAKARIAN, 2011, p.68).

Para fins de exemplificação, no auge do conflito, seis *botnets* diferentes foram utilizados para realizar ataques de *DDoS* na Geórgia. Diversos computadores de usuários desinformados foram utilizados, mas tiveram aqueles que também se voluntariam para que fossem instalados em seus computadores softwares piratas para deflagarem ataques aos sites da Geórgia (CLARKE; KNAKE, 2015), como um exército de milicianos cibernéticos voluntariados de diversas partes do mundo.

> O StopGeorgia.ru, por exemplo, fornecia ferramentas e instruções de fácil utilização para o lançamento de ataques de negação de serviço a partir de computadores particulares. Ele chegou a adotar um formato amigável bastante conhecido, um "botão" na tela onde se lia "INUNDAR". Este, quando "clicado", desencadeava vários ataques de negação de serviço contra alvos georgianos. Embora muitos desses ataques de hacktivistas dependessem de uma vulnerabilidade diferente com relação às ações de *botnet*, seu objetivo era igualmente sobrecarregar os servidores georgianos, empregando força bruta. As ferramentas fornecidas também eram muito versáteis. Por exemplo, alguns podiam atacar até 17 servidores georgianos ao mesmo tempo. (...) Também é importante citar que alguns especialistas em segurança conseguiram encontrar vínculos entre o StopGeorgia.ru e o crime organizado russo (SHAKARIAN, 2011, p.69).

Como resultado dos ataques cibernéticos, o poder de resposta do exército georgiano ficou limitado em relação às operações cinéticas russas. Acrescente-se o fato de se ter uma assertividade em conduzir os ataques no campo de batalha e coordenar respostas efetivas com um sistema de comunicação sobrecarregado e deficitário. A impossibilidade de acesso a comunicados, a notícias e a informações oficiais dificultaram o entendimento do que estava sendo atacado no espaço cibernético e no espaço físico. Adicione também o impacto psicológico, que pode causar pânico e confusão na população local, por estarem sem acesso a informações confiáveis (HANDLER, 2012, p.224).

Para Giles (2011, p. 46) a Rússia fez na verdade uma "guerra da informação" cujo conceito é mais holístico do que uma tradução literal sugere. A ideia de realizar operações cibernéticas está entrelaçada com disciplinas como guerra eletrônica, guerra psicológica e influência e estratégia de comunicações. Em outras palavras, a Rússia enxergava as capacidades cibernéticas como ferramentas de guerra de informação, que combina "inteligência, contraespionagem, *maskirovka*[26], desinformação, guerra eletrônica,

[26] Reconhecido como sistema de camuflagem soviético, cujo objetivo é esconder do inimigo a verdadeira posição das tropas e dar-lhe uma falsa ideia disso e, assim, conduzi-lo em erro e forçá-lo a uma conclusão que não corresponde para a situação. Além disso, a camuflagem constitui o meio mais importante para

interferência nas comunicações, degradação da navegação de apoio, pressão psicológica e destruição da rede de dados do inimigo".

Nesse contexto, destaca-se o uso de operações para divulgação de informações, mais conhecida em inglês pelo termo *Information Operations*, pois no confronto russo-georgiano exerceu um impacto profundo na publicação de informações a fim de influenciar a opinião pública durante o conflito. A forma como a Rússia neutralizou a utilização da Internet pela Geórgia e de sua capacidade de se comunicar internacionalmente e com os seus próprios cidadãos, e aproveitando dessa situação, a Rússia passou a ditar o que era verdade sobre o conflito, sem a contra defesa por parte da Geórgia. Informações que se tornaram ponto crítico como uma vulnerabilidade em todo o espectro das operações militares. A busca da Rússia pelo domínio de todo esse espectro militar não foi um sucesso total, mas a sua campanha de Operação de Informações foi suficiente para permitir uma vitória do exército russo (BARKER; FERMAINT; NEFF, 2013, p.22).

> Ao acusar o líder Mikhail Saakashvili para a comunidade internacional de crimes de guerra e tentativa de genocídio, Moscou pôs em risco a sua política de reaproximação com o Ocidente. Além disso, ao desacreditar o Presidente Saakashvili, o outro objetivo desta operação de informação, visava isolá-lo do povo georgiano. A mensagem da mídia russa então distinguiu o "criminoso" Saakashvili do povo georgiano, para quem o presidente Medvedov professou sua amizade fraterna. A Rússia poderia assim esperar uma mudança regime, sem ter de intervir militarmente em território georgiano. Sem afirmar nexo causal, as eleições seguintes, em 2012, foram vencidas pelo partido da oposição que posteriormente processou vários membros do regime de Saakashvili por corrupção. Ao demonstrar a falta de vontade por parte da OTAN em proteger os seus parceiros na região, Moscou sinalizou aos restantes vizinhos que uma política de conciliação com a Rússia era desejável, sob o risco de incorrer na ira do Kremlin (CHIASSON, 2019, p.57).

Muito provavelmente, como mencionou Giles (2011, p. 52) sobre as tropas da informação, o conceito russo de guerra da informação passou por uma categorização de diferentes tópicos, formada por "diplomatas, especialistas, jornalistas, escritores, publicitários, tradutores, operadores, comunicações pessoais, web designers, *hackers* e outros".

> Para construir uma rede de contramedidas de informação, é necessário desenvolver um centro de informação para determinar a criticidade e a importância da informação à respeito do inimigo, inclusive como eliminá-los psicologicamente, e como conduzir uma guerra eletrônica, uma guerra psicológica, um sistema de contrapropaganda e operações

---

alcançar a surpresa, que é uma das condições básicas para sucesso na batalha." Camuflagem é definida como "um tipo de suporte para as operações de combate e o cotidiano das tropas; um conjunto de medidas projetado para enganar o inimigo no que diz respeito à presença e disposição de tropas, várias instalações militares, seu status, combate prontidão e operações, bem como os planos do elemento de comando (KEATING, 1981, p.04).

> de rede que inclua treinamento de *hacker* (BBC MONITORING *apud* GILES, 2011, p. 52).

As unidades de inteligência russa fizeram o reconhecimento de sites importantes e infiltraram-se nas redes militares da Geórgia e nas redes governamentais em busca de dados úteis para a realização dos ataques. Esses ataques interromperam a transmissão de informações entre unidades militares e entre gabinetes do governo georgiano. Forças cibernéticas russas aproveitaram para atacar a rede de Internet em locais próximos de onde estavam ocorrendo as operações cinética com a finalidade de criar pânico entre a população civil. Moscou utilizou milícias cibernéticas russas, *hackers* irregulares de fora do governo com o objetivo de dar apoio às operações táticas militares e governamentais. Foi um período que tanto o governo quanto às milícias cibernéticas atuaram para desestruturar o espaço cibernético georgiano. Foram realizados ataques aos fóruns de *hackers* da Geórgia, a fim de evitar uma resposta retaliatória contra alvos russos (HADDICK, 2018, p.2).

Segundo o relatório realizado em agosto de 2009 pela Unidade de Consequências Cibernéticas dos Estados Unidos (em inglês *U.S. Cyber Consequences Unit* - US-CCU) (2009, p. 7), a resposta de defesa cibernética da Geórgia se baseou nas seguintes ações:

> 1. Contactar autoridades da Estônia que já tinham experiência em realizar campanhas de ataques cibernéticos. Essas autoridades colocaram os georgianos em contato com especialistas em cibersegurança internacionais de redes informais que eram capazes de oferecer orientações e apoio sobre o assunto. Mesmo tendo sido expressivo a quantidade de talentos georgianos no envolvimento informal na defesa cibernética da Geórgia, não conseguiram apoio de nenhuma organização internacional disponível para ajudar.
> 2. As técnicas iniciais de reposta aos ataques cibernéticos foi de instalar filtros que pudessem bloquear os endereços de IP vindo da Rússia e determinados protocolos usados pelos atacantes, mas infelizmente essas contra medidas foram contornadas pelos hackers usando endereços de IP de servidores localizados no estrangeiro.
> 3. A técnica de defesa cibernética que obteve resultados efetivos foi o de alterar o endereço dos sites da Geórgia e hospedá-los em outros países, onde o tráfico de ataque pudesse ser mais facilmente bloqueado e cuja banda de Internet fosse grande suficiente para segurar futuros ataques cibernéticos. Alguns dos websites do governo da Geórgia foram movidos para servidores na Estônia e nos

> Estados Unidos. Mesmo sendo empresas de hospedagem estrangeira e apesar de terem uma banda de Internet expressiva, houve muita dificuldade para manter acessível os sites da Geórgia, por causa o volume alto de tráfego gerado pelos atacantes nesses novos endereços de IP.
>
> 4. Houve apenas um contra-ataque cibernético georgiano significativo realizado contra alvos russos, mas o dano gerado foi muito limitado. Esse contra-ataque foi disposto em uma ferramenta de ataque hospedada em websites da Rússia com instruções para simpatizantes pró-russos usassem contra a Geórgia. O US-CCU obteve uma cópia dessa ferramenta e analisou e encontrou um procedimento de ataque designado para atacar somente websites russos, sendo 19 deles alvos pré-definidos. Qualquer simpatizante pró-russo que fez uso dessa ferramenta não tinha conhecimento que estava na verdade atacando os sites russos. Não se conseguiu nenhuma evidência de dano da utilização dessa ferramenta de ataque, o que sugere que nenhum dano significativo foi alcançado (US-CCU, 2009, p.07).

Mesmo com todas essas informações disponíveis, não se pode comprovar ao certo o envolvimento da Rússia nos ataques cibernéticos à Geórgia, devido à dificuldade de se localizar com exatidão de quais redes de computadores partiram esses ataques. Por esse motivo, Moscou mantém a sua versão de negar qualquer envolvimento no “apagão” cibernético da Geórgia (BARKER, FERMAINT, NEFF, 2013, p.5). Assim como no caso da Estônia, o governo russo alegou que os ciberataques eram uma resposta popular e que estavam fora do controle do Kremlin (CLARKE; KNAKE, 2015).

Sem uma confirmação oficial por parte do governo da Rússia, um grupo de peritos da computação concluiu que os ataques eram conectados ao aparato da inteligência russa. A orquestração e a coordenação do ataque, bem como o financiamento empregado, sugerem não ser uma cruzada cibernética qualquer, causada apenas por um nacionalismo patriótico. Ainda que se acreditasse que ataque cibernético à Geórgia, assim como a precedente sobre a Estônia não fosse trabalho de agentes oficiais russos, evidenciou-se que o Moscou não atuou para encerrar o ataque de negação de serviço do país vizinho. Infere-se que, dificilmente, atividades cibernéticas de larga escala na Rússia, sejam feitas pelo governo, pelo crime organizado ou por cidadãos, que não sejam de conhecimento e concesso do serviço de inteligência russa e dos superiores no Kremlin (CLARKE; KNAKE, 2015).

As técnicas e abordagens atualmente expostas representam a culminação de um processo evolutivo na guerra de informação russa tanto na parte teoria como na prática. Buscou-se reviver técnicas soviéticas bem estabelecidas de subversão e desestabilização e atualizá-los para a era da Internet. Seja pelo uso inovador das redes sociais como canais de comunicação digital, os métodos atuais russos têm raízes profundas na prática soviética de longa data. Após o fim da Guerra Fria, as práticas russas de guerra de informação causaram surpresa generalizada (GILES, 2016, p.33).

Para Barker, Fermaint e Neff (2013, p. 22) a Rússia deve ser reconhecida como líder em CNO (*Computer Network Operations*), por utilizar de forma eficaz as técnicas de MILDEC (*Military Deception*) ou *maskirovka* e OPSEC[27] (*Operation Security*), pois era um país até pouco tempo considerado atrasado em termos de guerra eletrônica (*Eletronic Warfare - EW*), mas foi eficaz no emprego de operações psicológicas (*Psychological Operations - PSYOP*) que paralisou a Geórgia e aliados georgianos por tempo suficiente para prevalecer na Guerra dos Cinco Dias.

> As operações em redes de computadores (CNO) podem ser consideradas um fenômeno relativamente novo, referente à guerra moderna. A operação da rede de computadores é composta por três componentes: ataque à rede de computadores (CNA), exploração da rede de computadores (CNE) e defesa da rede de computadores (CND). Ataque a redes de computadores é definido como operações para interromper, negar, degradar ou destruir informações residentes em redes de computadores, ou nos próprios computadores. A exploração de redes de computadores é a coleta realizada de forma inteligente e a habilitação de operações para coletar dados de sistemas de informação automatizados de adversários (AIS) ou redes. Finalmente, a defesa da rede de computadores são aquelas medidas, internas à entidade protegida, tomadas para proteger e defender informações, computadores e redes contra perturbações, degradação ou destruição. A guerra já não está limitada ao uso de armas cinéticas e métodos convencionais de guerra. As operações de redes de computadores tornaram-se parte integrante do arsenal dos adversários e deve ser dada mais atenção aos efeitos das atividades da CNO, particularmente da CNA e da CNE conduzidas pelos nossos adversários. Dos muitos estados suspeitos de conduzir atividades ativas da CNO contra os Estados Unidos e outras nações, nenhum merece mais atenção do que a Coreia do Norte (BROWN, 2004).

A guerra de agosto de 2008 entre a Geórgia e a Rússia serviu de exemplo quanto à influência da guerra de informação (*Information Warfare - IW*) para as autoridades russas. Foram expostas diversas deficiências nas forças armadas russas em relação ao armamento de guerra, principalmente as ferramentas baseadas em informação. O conflito

[27] A segurança operacional (OPSEC) é um processo contínuo usado para controlar informações. Abrange outras disciplinas de segurança, como segurança física, segurança da informação (INFOSEC), segurança informática (COMPUSEC) e segurança de comunicação (COMSEC) utilizadas para identificar e proteger informações críticas. A segurança operacional disciplinada (OPSEC) é observada rotineiramente entre unidades e tropas russas. A doutrina do engano militar russo (MILDEC) reconhece que atividades e eventos mesmo que benignos podem fornecer pistas que podem alertar um adversário (BARKER; FERMAINT; NEFF, 2013, p.16).

propiciou um alerta para a necessidade de inovação tecnológica e para uma reforma militar russa que certamente incluiria os mais recentes avanços na área de informática. O conflito com a Geórgia colaborou para elaboração de uma estratégia russa para a imersão na sociedade da informação em 2008 e para a elaboração de uma estratégia de segurança nacional em 2009 (BARKER; FERMAINT; NEFF, 2013, p.22).

Um dos pontos necessários a ser analisado em relação ao conflito cibernético entre a Rússia e a Geórgia se refere à abordagem do direito internacional atual quanto à a guerra cibernética e á neutralidade cibernética, que ainda não são tratadas de forma clara e explícita. A comunidade internacional não tem uma posição convicta se técnicas cibernéticas como DDoS são legalmente consideradas armas e se os ataques cibernéticos podem ser considerados atos legítimos de um conflito cinético. Software malicioso, ou malware, não é considerado armamento de guerra, mas os efeitos dos ataques cibernéticos podem ter um potencial de alcance semelhante ao armamento de guerra convencional. Um ataque cibernético que acarrete danos físicos à população e à infraestrutura crítica de um país pode ser entendido como um ataque com uso de armamento de guerra de acordo com a Carta das Nações Unidas. Para *International Telecommunication Union* (ITU), uma agência especializada em tecnologias de informação e comunicação da ONU, postula que os ataques cibernéticos poderiam, em teoria, ser considerados atos de guerra e serem tratados no âmbito do controle de armas ou das leis de conflito cinético (KORNS; KASTENBERG, 2008, p.63).

> ARTIGO 51 - Nada na presente Carta prejudicará o direito inerente de legítima defesa individual ou coletiva no caso de ocorrer um ataque armado contra um Membro das Nações Unidas, até que o Conselho de Segurança tenha tomado as medidas necessárias para a manutenção da paz e da segurança internacionais. As medidas tomadas pelos Membros no exercício desse direito de legítima defesa serão comunicadas imediatamente ao Conselho de Segurança e não deverão, de modo algum, atingir a autoridade e a responsabilidade que a presente Carta atribui ao Conselho para levar a efeito, em qualquer tempo, a ação que julgar necessária à manutenção ou ao restabelecimento da paz e da segurança internacionais (ONU, 1948).

As leis internacionais de guerra existentes baseiam-se geralmente na noção de “fronteiras”, na medida em que essas leis regem principalmente os conflitos entre Estados-nação com fronteiras geográficas reconhecidas. Esta construção é fundamentalmente fraca na abordagem da participação de atores não estatais e de não existir fronteiras em caso de conflitos cibernéticos em que os indivíduos organizam as suas próprias campanhas de ataques cibernéticos.

Os governos georgiano e russo eram combatentes convencionais no conflito da Ossétia. Existe dúvida se seriam também combatentes cibernéticos. É mais fácil identificar as partes quando se consegue captar a explosão de bombas e tiros de artilharia, mas não é o caso das atividades cibernéticas. Ambos os governos negam a participação de terem executados ataques cibernéticos de *DDoS*, possivelmente eram ataques cibernéticos por procuração, e não ataques diretos entre nações. Ataques cibernéticos advindos por procuração podem ser realizados por criminosos cibernéticos, ou por milhares de pessoas conectadas à Internet de diversas partes do mundo ou por milícias cibernéticas. Esta distinção leva à incerteza de quais partes foram ciberneticamente atuantes. Tanto o caso da Geórgia quanto da Estônia em 2007, serviram para expor um conflito de uma nação contra um inimigo anônimo. O que se entendia por guerra cibernética teve o seu conceito na retrospectiva de análise do pós-conflito modificado, a comunidade internacional parece ter chegado a um consenso que os ataques *DDoS* não atribuíveis e não estatais não são necessariamente uma guerra cibernética, mas possíveis atos de terrorismo, o que não deixa de ser um crime (KORNS; KASTENBERG, 2008, p.70).

2.3. Caso 3: Stuxnet (2010)

Stuxnet é um *worm* de computador que foi projetado e implantado para atacar as instalações nucleares iranianas (BUXTON, 2022), desenvolvido não para espionagem, mas para sabotar as centrífugas, cujo principal objetivo era parar ou atrasar o programa nuclear do Irã (BAEZNER; ROBIN, 2017, p.04). Ele foi descoberto em um computador na instalação nuclear de Natanz no Irã, em 2010, responsável pelo enriquecimento de urânio daquela usina, causando prejuízo em suas centrífugas.

> O malware Stuxnet é frequentemente chamado de vírus, mas é classificado com mais precisão como um *worm*. Tanto os vírus quanto os *worms* são projetados para causar danos e interrupções, infectar sistemas, corromper arquivos e espalhr-se rapidamente. Mas, ao contrário dos vírus, que exigem um arquivo ou programa host para serem ativados e autorreplicarem-se, os worms são autossuficientes. Em outras palavras, os worms se autorreplicam sem precisar de entrada externa, como um arquivo ou programa host, tornando-os uma ameaça cibernética sofisticada e perigosa (BUXTON, 2022).

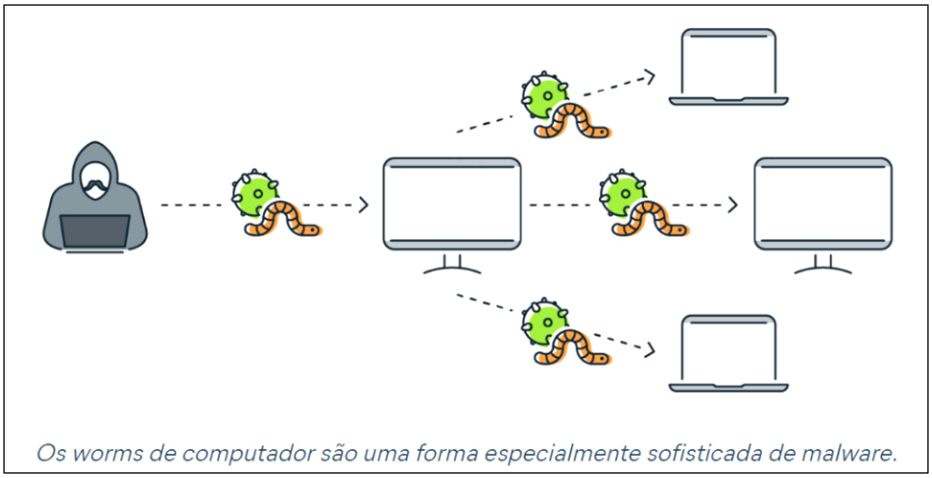
O malware Stuxnet foi a mais sofisticada arma cibernética já desenvolvida e aparentemente foi uma obra conjunta de diversos autores espalhados em vários continentes (TEIXEIRA, 2011).

> O sistema que o Stuxnet foi projetado para atacar um produto de sofware específico do fabricante alemão Siemens, algo chamado Siemens WinCC-7. O software da Siemens estava comercialmente disponível ao redor do mundo. O Siemens WinCC-7 era um sistema SCADA, um programa de Supervisão e Aquisição de Dados projetado para monitorar e enviar instruções para certos tipos de maquinaria. Os sistemas SCADA são mais bem conhecidos por dirigir máquinas essenciais em uma rede de energia elétrica (transformadores, geradores), mas eles também executam muitas outras coisas, incluindo linhas de montagem automatizadas, refinarias de petróleo e, sim, grandes conjuntos de centrífugas nucleares (CLARKE; KNAKE, 2015).

De acordo com o jornal norte-americano "*New York Times*", o projeto sigiloso contou com a parceria dos Estados Unidos, Israel, e de forma consciente ou não, da Alemanha e da Grã-Bretanha. Possivelmente, teria havido também a participação de empresas privadas, como a Siemens que repassou para o laboratório Nacional de Idaho, nos EUA, informações sobre as vulnerabilidades, conhecidas também como brechas de segurança do sistema utilizado para o enriquecimento do urânio que foram exploradas pelo Stuxnet (TEIXEIRA, 2011).

O worm Stuxnet foi considerado um malware de alta complexidade e uma novidade mundial em termos de ação, embora tenha sido projetado da mesma forma que qualquer outro worm malicioso projetado para se autorreplicar nas redes. Só que no caso do Stuxnet no Irã, ele foi usado para implantar *bots* a fim de assumir o controle de todas as configurações do sistema de controle industrial[28] da Usina (BUXTON, 2022).

Figura 22 - Worms de computador



Fonte: (BUXTON, 2022)

[28] Os sistemas de controle industrial são usados em gasodutos e usinas de energia. O objetivo final do Stuxnet era reprogramar sistemas de controle industrial (ICS), modificando o código em controladores lógicos (PLC´s) para fazê-los funcionar da maneira pretendida pelo invasor e para ocultar essas alterações do operador do equipamento (FALLIERE; MURCU; CHIEN, 2011, p.01).

Ao se infiltrar nas instalações de enriquecimento nuclear do Irã, figura 22, o Stuxnet saiu em busca de computadores conectados aos controladores lógicos programáveis (PLC) que interagem e controlam os motores das centrífugas envolvidas na produção de material nuclear para armas (BUXTON, 2022). O worm alterou o código dos PLCs para forçar uma mudança na velocidade do rotor da centrífuga, primeiro aumentando a velocidade e depois reduzindo, provavelmente com a intenção de induzir vibrações ou distorções excessivas para destruir a centrífuga. Ainda segue de forma desconhecida as sequências de ataque e possíveis respostas do sistema de controle industrial da Usina de Enriquecimento de Combustível. Estas respostas poderiam atuar durante o ataque para reduzir a magnitude da mudança na frequência ou de outra forma agir para proteger as centrífugas. (ALBRIGHT; BRANNAN; WALROND, 2010, p.06 e 07).

> As centenas de centrífugas enterradas debaixo do solo de Natanz eram todas interligadas. Embaixo de cada centrífuga estava um motor elétrico poderoso e sofisticado. Cada motor fazia com que o urânio e o gás girassem em alta velocidade, certamente mais rápido do que a velocidade do som. É este girar que concentra e "enriquece" o urânio a concentrações utilizadas em armas. Os comandos para girar são enviados aos dispositivos de controle para motores elétricos, chamados PLC, ou controladores lógicos programáveis (CLARKE; KNAKE, 2015).

A finalidade do malware era penetrar nas redes de computadores e então procurar pelo software da Siemens WinCC-7. Caso não encontrasse, o Stuxnet não agiria e continuaria se movendo, penetrando outras redes. A técnica de penetração utilizada nunca tinha sido vista antes, e foi, portanto, chamada pelos *hackers* de "ataque zero-day ou ataque dia zero" (CLARKE; KNAKE, 2015).

Para atingir este objetivo, os criadores do Stuxnet reuniram um vasto conjunto de componentes para aumentar as suas chances de sucesso. Isso inclui o dia exploração como dia zero, um *rootkit* do Windows, o primeiro *rootkit* PLC, evasão de técnicas de antivírus, injeção de processos complexos e código de conexão, rotinas de infecção de rede, atualizações ponto a ponto e uma interface de comando e controle (FALLIERE; MURCU; CHIEN, 2011, p.01 e 02).

> Um *rootkit* é um tipo de malware projetado para dar aos *hackers* acesso e controle sobre um dispositivo. Embora a maioria dos *rootkits* afete o software e o sistema operacional, alguns também podem infectar o hardware e o firmware do seu computador. Os *rootkits* são especializados em ocultar a sua presença, mas enquanto permanecem escondidos, eles estão ativos. Uma vez que eles ganham acesso não autorizado a computadores, os *rootkits* permitem que os criminosos cibernéticos roubem dados pessoais e informações financeiras, instalem malware ou usem os computadores como parte de uma *botnet* para circular mensagens de spam e participar em ataques DDoS (ataque de negação de serviço). O nome "*rootkit*" deriva dos sistemas operacionais Unix e Linux, onde o

> administrador de contas mais privilegiado é chamado de "root". Os aplicativos que permitem o acesso não autorizado de raiz ou a nível administrativo ao dispositivo são conhecidas como o "kit"(KASPERSKY, 2023c).

"Dia zero" é um termo amplo que descreve as vulnerabilidades de segurança recentemente descobertas que os *hackers* podem usar para atacar sistemas. Nesse caso o fornecedor ou desenvolvedor acabou de conhecer a falha, e por isso tem "zero dias" para corrigi-la. Esse tipo de ataque ocorre quando *hackers* exploram a falha antes que os desenvolvedores tenham a chance de lidar com ela. As palavras vulnerabilidade, exploração e ataque são normalmente usadas em conjunto com o dia zero e são úteis para entender a diferença entre esses termos:

- Uma vulnerabilidade de dia zero é uma vulnerabilidade de software descoberta por invasores antes que o fornecedor tome conhecimento dela. Como os fornecedores não a conhecem, não existe correção para vulnerabilidades de dia zero, o que aumenta a probabilidade de o ataque ser bem-sucedido.
- Uma exploração de dia zero é o método que os *hackers* usam para atacar os sistemas com uma vulnerabilidade não identificada anteriormente.
- Um ataque de dia zero é o uso de uma exploração de dia zero para causar danos ou roubar dados de um sistema afetado por uma vulnerabilidade (KASPERSKY, 2023d).

O Stuxnet tinha capacidade de trabalhar de duas formas distintas. Uma funcionalidade era fazer com que as centrífugas nucleares do Irã girassem descontroladamente. A outra funcionalidade parecia ter saído das telas do cinema, o malware gravava secretamente como eram as operações normais na usina nuclear e depois reproduzia essas leituras para os operadores da usina, como uma fita de segurança pré-gravada em um assalto a banco, para que parecesse que tudo estava funcionando normalmente enquanto as centrífugas estavam girando de forma descontrolada (BROAD; MARKOFF; SANGER, 2011). A figura 23 mostra uma foto via satélite da planta de enriquecimento de urânio em Natanz – Irã.

Figura 23 - Imagem de satélite (2002) da planta de Natanz - Irã

Fonte: (ZETTER, 2011)

É importante compreender o contexto histórico e a cronologia dos acontecimentos (ver Apêndice B) que antecederam a descoberta do *worm* Stuxnet e suas subsequentes investigações, pois o Stuxnet foi desenvolvido e usado contra o programa nuclear iraniano em um momento de grandes tensões existentes entre o Irã e os EUA. A tentativa do Irã de desenvolver energia nuclear e possivelmente armas nucleares, gerou um ambiente de grande tensão entre esses dois países. A situação se agravou a ponto de Israel, inimigo declarado do regime do Irã, preparar-se para intervir militarmente com a finalidade de impedir o Programa Nuclear Iraniano (BAEZNER; ROBIN, 2017).

Sergey Ulasen foi considerado a pessoa quem descobriu o *worm* da Stuxnet pela primeira vez. Relata-se que em junho de 2010, quando trabalhava em seu escritório na Bielorrússia a examinar e-mails, leu uma reportagem que chamou sua atenção. Um computador pertencente a um cliente no Irã foi apanhado num ciclo de reinicialização, desligando e reiniciando repetidamente, apesar dos esforços dos operadores para assumir o controle do computador (ZETTER, 2011).

Ulasen chefiava uma divisão de antivírus de uma pequena empresa de segurança de computadores em Minsk, capital da Bielorrússia, chamada VirusBlokAda. Antigamente a área de segurança de computadores era uma ramificação da Ciência da Computação, mas com o avanço da tecnologia tornou-se um mercado multibilionário após o crescimento de ataques de *hackers* e a evolução dos vírus, tais como cavalos de Tróia e programas de *spyware* (ZETTER, 2011).

A princípio, o suporte técnico do VirusBlokAda havia escaneado o sistema remotamente de Minsk em busca de malware em seu antivírus, mas o programa falhou e não encontrou nada. Foi quando acionaram Ulasen para investigar o problema (ZETTER, 2014).

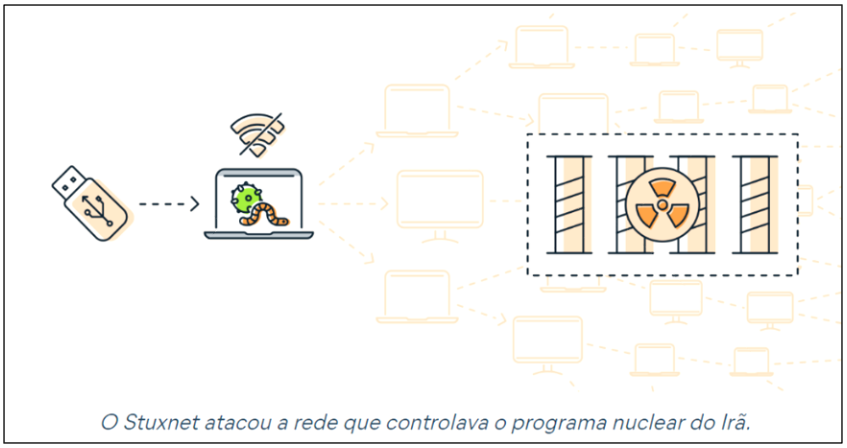
> Era uma tarde quente de quinta-feira, em que Ulasen chefiava a divisão de antivírus de uma pequena empresa de segurança informática na Bielorrússia chamada Virus-BlokAda. Ele estava sentado com o seu colega Oleg Kupreev em seu laboratório no centro de Minsk, dentro de um prédio monótono da era soviética, a cerca de um quarteirão do rio Svisloch. Eles estavam vasculhando metodicamente arquivos de computador suspeitos que tinham descoberto recentemente numa máquina no Irã, quando algo impressionante saltou sobre Kupreev. Ele recostou-se na cadeira e chamou Ulasen para dar uma olhada. Ulasen percorreu o código uma vez, depois novamente, para ter certeza de que ele estava vendo o que pensava ter visto. Um pequeno suspiro escapou de sua garganta. O código que eles inspecionaram nos últimos dias, algo que eles até agora consideravam um vírus moderadamente interessante, mas ainda assim comum, tinha acabado de revelar-se uma obra de gênio silencioso e diabólico (ZETTER, 2014).

Na análise do malware, verificou-se que o Stuxnet envolveu quatro ataques dia zero diferentes. Para os *hackers*, um ataque como Stuxnet foi considerado bem elaborado e sofisticado, algo para atingir um alvo específico, para uma situação especial. Era necessário que fosse secreto, para que ninguém descobrisse a vulnerabilidade do software e corrigisse antes da possibilidade de explorá-la. Para quatro ataques dia zero, se uma técnica não funcionasse, tentar-se-ia outra, então outra, então a quarta. Por isso que todo o trabalho realizado para a criação do Stuxnet tinha como objetivo entrar em algum software da Siemens WinCC-7, especificamente o da usina nuclear de Natanz (CLARKE; KNAKE, 2015).

Acredita-se que, como os sistemas de controle do Natanz não estavam conectados à Internet, o Stuxnet precisaria viajar em uma unidade removível, tipo um *pendrive*, de um computador infectado para o sistema de controle industrial de Natanz (vide figura 24). Os empregados da Usina de Natanz poderiam ter transportado o Stuxnet sem saber por meio de computadores pessoais infectados. Talvez os atacantes tivessem como primeiro alvo os computadores pessoais desses funcionários. O malware poderia ter levado meses

para chegar aos sistemas de controle da centrífuga Natanz (ALBRIGHT; BRANNAN; WALROND, 2010, p.02).

Figura 24 - O ataque do worm Stuxnet na Usina Nuclear do Irã



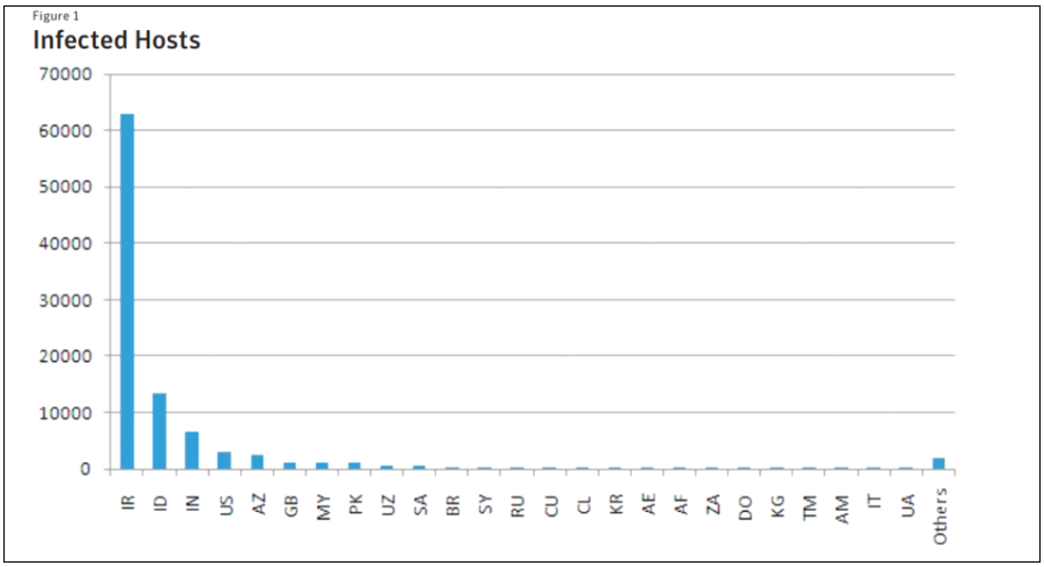
Fonte: (BUXTON, 2022)

Segundo a análise realizada por Albright; Brannan; Walrond (2010, p.01) no final de 2009 ou início de 2010, o Irã desativou e substituiu cerca de 1.000 centrífugas IR-1 na Fábrica de Enriquecimento de Combustível (em inglês *Fuel Enrichment Plant* - FEP) em Natanz, o que se deduziu que essas centrífugas apresentaram defeitos. Observaram que as centrífugas IR-1 do Irã quebravam frequentemente, mas não ao nível de serem tantas em um curto espaço de tempo, o que indicaria uma infecção do malware Stuxnet. Este código malicioso procurou dominar um sistema de controle industrial com fins de destruir equipamentos enquanto ocultava a sua presença. O Stuxnet alterou secretamente as frequências de certos tipos de conversores, que controlavam a velocidade dos motores das centrífugas.

> Se o objetivo do Stuxnet era a destruição de todas as centrífugas da FEP, o Stuxnet falhou. Mas se o seu objetivo fosse destruir um número mais limitado de centrífugas e atrasar o o programa de enriquecimento do urânio, enquanto o malware se manteve escondido, ele pode ter tido sucesso, pelo menos por um tempo (ALBRIGHT; BRANNAN; WALROND, 2010, p.01).

O gráfico a seguir mostra o número de hosts infectados por país:

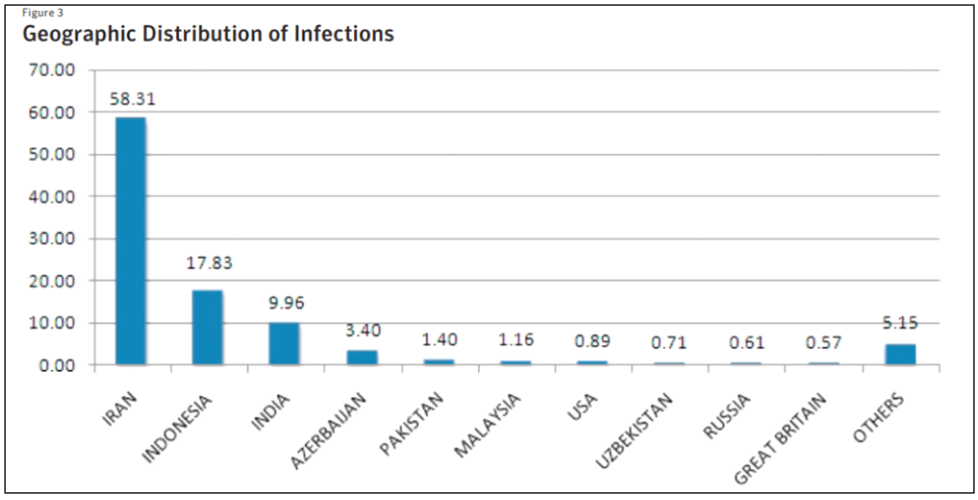
Gráfico 1 - Quantidade de Hosts infectados por país



Fonte: (FALLIERE; MURCU; CHIEN, 2011, p.05)

Foram mais de 40.000 endereços IP externos exclusivos, de mais de 155 países. Analisando a porcentagem de hospedeiros infectados por país, nota-se que aproximadamente 60% dos hospedeiros infectados estavam no Irã, gráfico 2:

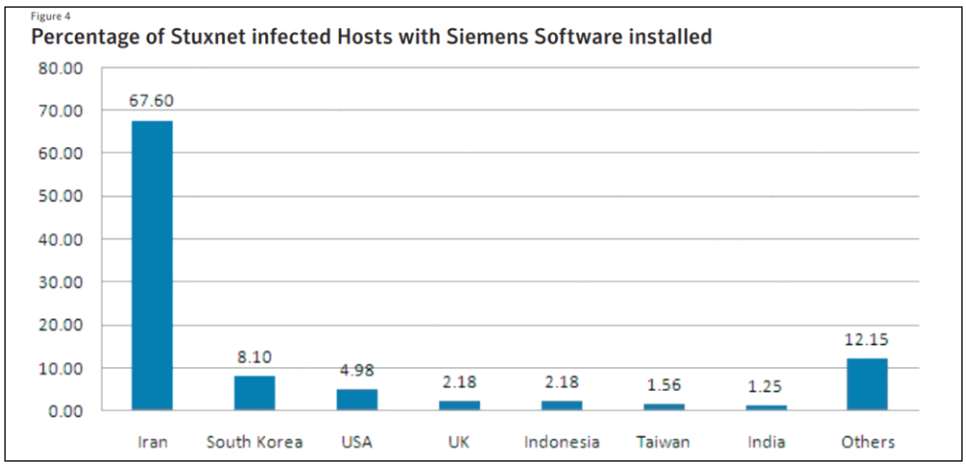
Gráfico 2 - Distribuição geográfica das infecções



Fonte: (FALLIERE; MURCU; CHIEN, 2011, p.06)

O Stuxnet tinha como objetivo identificar os hosts que possuíam o software Siemens instalado. O gráfico a seguir mostra a porcentagem de hosts infectados por país com o software Siemens instalado.

Gráfico 3 - Percentual de hosts infectados pelo Stuxnet com o software da Siemens instalado



Fonte: (FALLIERE; MURCU; CHIEN, 2011, p.06)

A conclusão que se pode encontrar é que o Stuxnet não foi um ataque único e isolado; foi uma campanha de destruição lenta que durou semanas e meses. O Irã declarou o Stuxnet como um ato de guerra eletrônica e tratou de conter o *worm* e removê-lo de suas redes. Mesmo assim, verificou-se que todos os esforços foram prejudicados pela capacidade do Stuxnet de sofrer mutações e continuar se espalhando. No final de 2010, autoridades iranianas admitiram publicamente que levaria vários meses para erradicar o *worm* de todos os sistemas (CLARKE; KNAKE, 2015).

Embora o Stuxnet tenha sido projetado para expirar em 2012, como se espalhou para fora das instalações inicialmente visadas, já não era mais segredo. Desde então, houve uma série de ataques cibernéticos adicionais à infraestrutura usando *worms* com características e recursos semelhantes ao Stuxnet (BUXTON, 2022).

2.4. Apagões no Brasil (2005/2007/2009) supostos ciberataques

Uma reportagem publicada pelo Portal Folha de São Paulo, no dia 08 de novembro de 2009, relatou que agentes de segurança e informação do governo dos Estados Unidos apresentaram indícios de que empresas de energia do Brasil sofreram ataques de hackers. Nesse mesmo dia, um programa jornalístico “60 Minutes”, da rede norte-americana CBS, informou que o apagão de 2007 no Estado do Espírito Santo, que afetou mais de três milhões de pessoas, e um incidente menor no Rio de Janeiro, em 2005, tinham sido causados por hackers (FOLHA, 2009a).

De acordo com o programa da CBS, quatro meses após assumir o cargo, o presidente americano, Barack Obama, em um discurso, afirmou que a infraestrutura digital dos Estados Unidos era um ativo estratégico e afirmou que a guerra cibernética tinha saído do campo da teoria para a prática. Obama citou ataques que invasores cibernéticos estavam sondando a rede elétrica americana e que outros países ficaram sem energia elétrica em razão de ataques cibernéticos. A referência a "outros países" feita pelo chefe da Casa Branca incluía o Brasil (FOLHA, 2009a).

Dois dias após a reportagem do "60 minutes" ir ao ar, o Brasil sofreu outro apagão elétrico, que atingiu parte do Brasil e do Paraguai (FOLHA, 2009b). A coincidência fez surgir novas suspeitas sobre a ação de hackers.

No entanto, órgãos brasileiros não confirmaram as informações apresentadas pelo governo americano. O Brasil alegou que não havia provas que o apagão de 2009, bem como os de 2005 e 2007 tenham sido causados por ciberataques. O ministro de Minas e Energia, Edison Lobão, à época, não quis comentar a possibilidade de o apagão ter sido causado por algum *hacker*. Furnas também negou (VALLE, 2009).

Segundo a empresa Furnas, em 2007, a causa do apagão foi a poluição acumulada sobre os cabos de energia por conta da falta de chuvas na região que enfrentava uma estiagem por cerca de oito meses. O ex-presidente da Eletrobrás, Luiz Pinguelli Rosa, afirmou em entrevista à GloboNews não acreditar que o apagão tenha sido causado por algum tipo de sabotagem. Posteriormente, acrescentou que, aparentemente, não havia danos físicos no sistema, como a queda de uma torre por um raio. O diretor da Itaipu, Jorge Samek, informou que o apagão poderia ter sido causado por alterações climáticas (VALLE, 2009).

No entanto, diversos especialistas criticaram o programa da CBS por falta de provas. Uma reportagem publicada pela revista norte-americana "Wired", que entrevistou Richard Clark, um ex-assessor especial no governo de George W. Bush também mencionou o Brasil, como país que sofreu ataque cibernético em sua matriz energética, mas sem apontar nenhuma evidência concreta. A revista citou que o governo brasileiro e a empresa de energia local, Furnas, negaram a alegação da CBS News e que, conforme publicado no jornal da Folha, o diretor do Departamento de Segurança da Informação e Comunicação do Gabinete de Segurança Institucional da Presidência da República, Raphael Mandarino, havia informado que a investigação brasileira não encontrou evidências de ataques de hackers. Mandarino acrescentou que o sistema de controle de energia elétrica não estava diretamente conectado à Internet, o que dificultaria um *hacker*

entrar na rede interna. A revista criticou o fato de no programa da CBS não ter mencionado na transmissão a contestação do governo brasileiro e da Companhia de Energia (POULSEN, 2009).

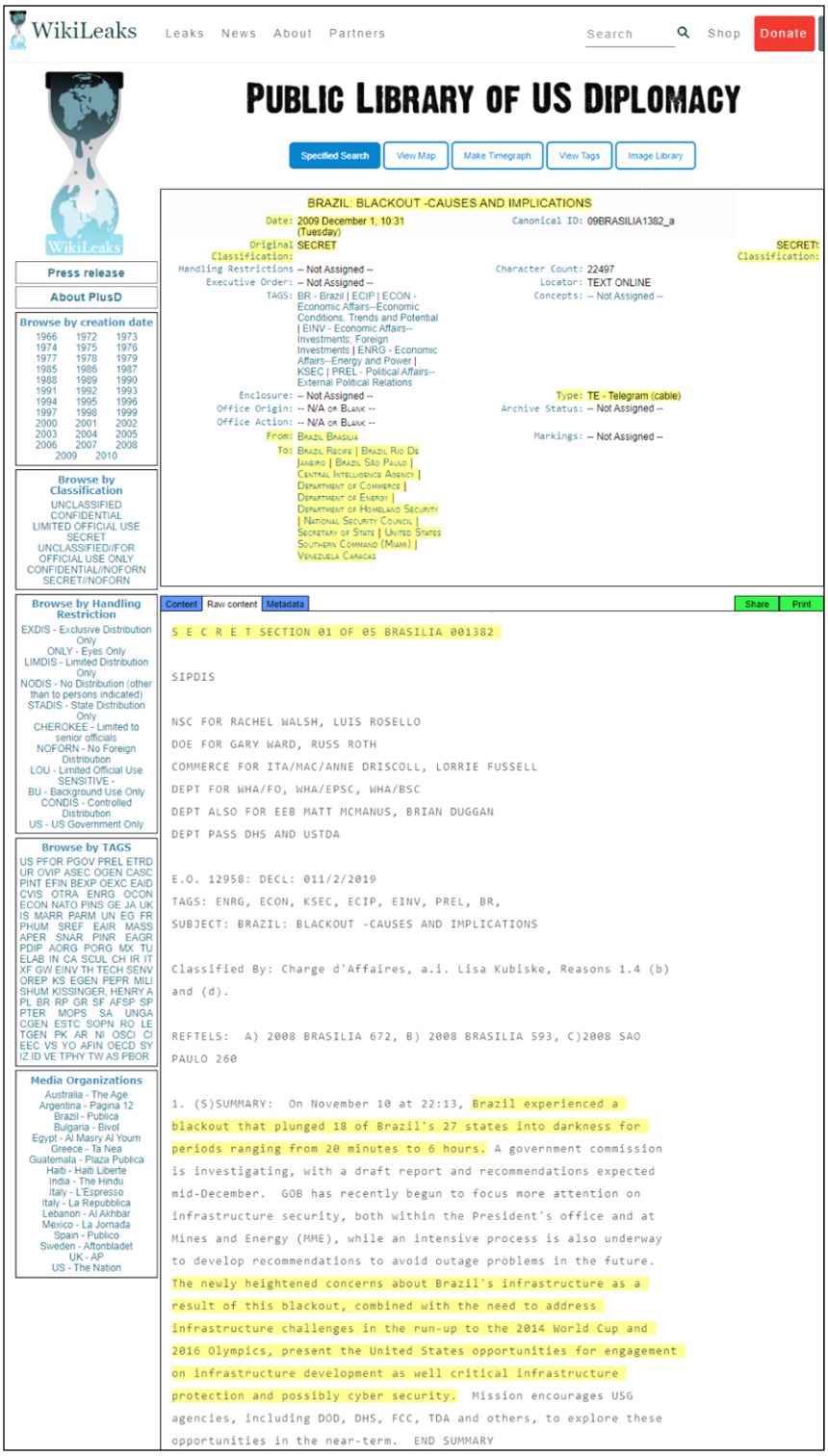
A revista Wired voltou a publicar uma nova matéria depois da apresentação do programa da CBS News, cujo apagão de 2007 no Brasil não tinha sido realizado por *hackers*, mas que na verdade foi resultado de negligência na manutenção dos isoladores de alta tensão em duas linhas de transmissão e que a causa do apagão estava em conformidade com os relatórios dos órgãos reguladores do governo brasileiro que investigaram o incidente por mais de um ano (SOARES, 2009).

Um ano depois, um vazamento do *Wikileaks*[29] contendo telegramas secretos enviados pelo Brasil ao governo norte-americano revelou uma análise das causas desse apagão. Realmente, a possibilidade de um ataque hacker foi descartada pelas autoridades brasileiras.

Classificado como "secreto", o texto relatou conversas da Embaixada Americana com técnicos brasileiros do Operador Nacional do Sistema Elétrico (ONS) e do Ministério de Minas e Energia (vide figura 25). O apagão de 2009 havia provocado a interrupção na transmissão de 28.800 Megawatts de energia no Brasil e de 980 Megawatts no Paraguai. O incidente ocorreu na transmissão entre Foz de Iguaçu (PR) e Tijuco Preto (SP), provocando um efeito cascata nos sistemas de transmissão e subtransmissão de São Paulo, Rio de Janeiro e Espírito Santo. No total, 18 estados foram afetados.

[29] Em 2010, o site *Wikileaks* criado quatro anos antes divulgou centenas de milhares de documentos secretos do governo americano. Relatórios da atuação militar no Afeganistão e no Iraque revelaram abusos de direitos humanos, mortes de civis, crimes de guerra. Telegramas diplomáticos trouxeram à tona os bastidores de temas sensíveis na relação com outros países. Governos reagiram. O site chegou a sair do ar. Doações foram bloqueadas. Mas logo o alvo principal passou a ser o criador do Wikeleaks, Julian Assange, programador e ativista australiano (MOREIRA, 2023).

Figura 25 - Parte da cópia do documento vazado da Wikileaks



Fonte: (WIKILEAKS, 2009)

No texto, a embaixada americana informou sobre a preocupação do governo brasileiro sobre a segurança em razão da Copa de 2014 e das olimpíadas de 2016 e que o

incidente chamou a atenção para possíveis vulnerabilidades no sistema elétrico (ROHR, 2019).

> Dois dias após o incidente, segundo uma fonte confiável, autoridades de segurança no Brasil atribuíram a interrupção a "erros humanos" por parte do operador de sistema. Segundo a fonte, aquele operador estava sob investigação. A fonte não está disponível para comentários adicionais pois a evolução das análises pode afetar essa hipótese e o status dessa investigação específica segue desconhecida. Houve também especulação privada em pelo menos uma conversa entre funcionários do governo, aparentemente baseados em parte na coincidência "60 Minutos programa" poucos dias antes, sugerindo vulnerabilidades no sistema brasileiro, que os interesses do setor privado dos EUA podem ter planejado os apagões para obter melhor acesso comercial à grade do programa (WIKILEAKS, 2009).

Em 2010, a Secretaria de Assuntos Estratégicos da Presidência da República, em parceria com o Comando do Exército e por meio do Estado-Maior do Exército, realizou no dia 16 de dezembro de 2010, na cidade de Brasília, uma Reunião Técnica sobre Segurança e Defesa Cibernética (BARROS; GOMES; FREITAS, 2011, p.09). O evento buscou atingir dois objetivos principais:

1 - Proporcionar aos servidores do governo federal conhecimento sobre as atividades de segurança e defesa cibernéticas, identificando o papel desenvolvido pelas Forças Armadas e de outras instituições do Estado brasileiro na área, bem como de outros órgãos públicos e privados envolvidos ou relacionados ao tema.

2 - Contribuir para capacitar os órgãos públicos a propor políticas públicas que considerem a indissolubilidade do binômio defesa–desenvolvimento, permitindo ao país estabelecer um sistema de segurança e defesa cibernéticas que envolva também os sistemas de informação ligados às infraestruturas críticas (BARROS; GOMES; FREITAS, 2011, p.09).

Foram apresentados diagnósticos dos assuntos em debate e os desafios mais relevantes no que tange aos seguintes aspectos:

- a formulação de políticas públicas e de marco legal para o uso efetivo do espaço cibernético, especialmente no que concerne à manutenção das infraestruturas críticas do País;
- o estabelecimento de medidas que contribuam para a gestão da segurança da informação e comunicações e para a produção do conhecimento de inteligência;
- o estímulo das atividades de pesquisa e desenvolvimento para atender às necessidades do setor; a retenção de talentos; e
- o estabelecimento do perfil da carreira que deve ser de Estado.

O documento final da reunião técnica propôs a criação e a implementação de um grupo de trabalho do Setor Estratégico Cibernético, a ser constituído pela Secretaria de Assuntos Estratégicos, em parceria com o Ministério da Defesa, especialmente no que tange à criação do Sistema de Segurança e Defesa Cibernético brasileiro (BARROS; GOMES; FREITAS, 2011, p.10).

3. Grandes eventos internacionais sediados no Brasil

A importância do tema quanto aos ataques cibernéticos com motivação política aumentou significativamente após os incidentes ocorridos na Estônia (2007) e Geórgia (2008), duas ex-repúblicas soviéticas que buscavam uma aproximação com o Ocidente, com consequentemente distanciamento da esfera de influência russa. Ambos os países sofreram ataques cibernéticos que impediram o funcionamento da infraestrutura de rede de dados, como serviços financeiros, de telecomunicações e o funcionamento da máquina governamental. O padrão dos ataques foi muito semelhante e tudo apontava a Rússia como responsável.

Em 2010, o Irã sofreu um ataque virtual que atrasou seu programa nuclear. Um programa malicioso chamado Stuxnet (2009), conforme tratado no capítulo 2, projetado especificamente para atacar o sistema operacional usado nas centrífugas de enriquecimento de urânio do país e danificá-las. O programa, detectado por especialistas da Bielorrússia em junho de 2010, foi escrito para atacar o sistema industrial SCADA e causar danos no funcionamento dos geradores, obrigando os iranianos a adiar o desenvolvimento de seu programa nuclear.

A sofisticação dos ataques cibernéticos permite que hoje em dia se paralisem setores inteiros da economia de um país. Os danos gerados com as invasões virtuais na Estônia e na Geórgia motivaram vários governos a tratarem o assunto como questão de segurança nacional. O Brasil foi um deles. A possibilidade de ser alvo de ataques virtuais motivou o Ministério da Defesa a criar, em 2010, o Centro de Defesa Cibernética (CDCiber), vinculado ao Ministério da Defesa. Uma das atribuições do órgão é monitorar o potencial negativo das ameaças virtuais (INOHARA, 2011).

Na abertura do primeiro dia da VIII Conferência Internacional de Perícias em Crimes Cibernéticos (ICCyber), realizada de 5 a 7 de outubro de 2011, em Florianópolis, com representantes do Exército Brasileiro, da Polícia Federal, do Serviço Federal de Processamento de Dados (SERPRO) e da Presidência da República, foi realizado um

debate intitulado: "Estratégias de governo para prevenção e combate a ataques cibernéticos". O debate explanou sobre as atividades de monitoramento de informações coletadas em diversas esferas da sociedade e a integração entre os órgãos de defesa do Governo Federal (SERPRO, 2011).

> A ICCyber é um dos mais importantes eventos de tecnologia e perícias em informática existentes na América Latina, contando com uma agenda completa de palestras com conteúdo técnico-científico, assim como uma programação estruturada por Peritos Criminais Federais da área de Informática, de renomados especialistas e consultores, acadêmicos de diversas universidades brasileiras e internacionais, de executivos de importantes corporações de base tecnológica, além de instituições de representação da sociedade civil brasileira e internacional (HARDWARE, 2011)

Em relação a monitoração estratégica, os debatedores trataram de forma unânime a necessidade de um constante trabalho no sentido de colher todo o tipo de informação para antever ataques a informações sigilosas e sabotagens em redes de informação e comunicação. Na época, o Coordenador Geral de Informação do SERPRO, Ulysses Machado, destacou a necessidade de o Governo Federal manter uma estrutura adequada, mapeamento de riscos e um plano de continuidade para a monitoração estratégica adequada (SERPRO, 2011).

Quanto à cooperação entre as instituições, verificou-se a necessidade de manter uma constante evolução técnica do pessoal operacional e dos órgãos de defesa de informações brasileiros para a troca de informações entre si, pois os *hackers* ao redor do mundo contam com a contínua evolução tecnológica ao seu favor, o que se torna uma desvantagem para os governos ao não se atualizarem com as tendências da sociedade e das novidades tecnológicas (SERPRO, 2011).

Destacou-se a segurança cibernética para os grandes eventos internacionais (Rio +20, Copa do Mundo e Olimpíadas) sediados pelo Brasil. No caso dos grandes eventos, foi informado na conferência que eles costumam atrair a atenção de um grande número de pessoas, e por isso torna-se um interessante alvo de ataques, seja nos sistemas do governo, como nos privados. A exemplo de um ataque no sistema de cobrança *on line* ou no fornecimento de água durante um evento (SERPRO, 2011).

3.1. RIO +20 (2012)

Rio +20 foi a Conferência das Nações Unidas sobre Desenvolvimento Sustentável realizado na cidade do Rio de Janeiro nos dias 13 a 22 de junho de 2012, onde milhares de participantes de governos, do setor privado, de ONGs e de outros parceiros

interessados se reuniram para um forte impulso na direção do desenvolvimento sustentável (ONU, 2012).

Foi um dos grandes eventos realizados no Brasil, cujo objetivo foi a busca por soluções para muitos problemas do desenvolvimento sustentável, incluindo desafios relacionados a cidades, energia, água, alimento e ecossistemas (ONU, 2012).

De acordo com o portal de notícias G1, o evento contou com um forte aparato de segurança montado para a realização da cúpula, considerado o maior já realizado pela ONU, com a participação de cerca de 20.000 pessoas e com equipes para evitar ataques cibernéticos e terroristas. Foram investido 64,5 milhões de dólares para combater ataques cibernéticos e terroristas, uma unidade de 40 especialistas e uma infraestrutura foi montada para proteger o sistema de telecomunicações de qualquer ataque de *hackers* (G1, 2012).

O coordenador de Segurança da Rio+20, na época o comandante militar do Leste, general Adriano Pereira Júnior, informou que o exército comandou o Centro de Monitoramento Cibernético, com a ajuda da Abin, Polícia Federal e Polícia Civil, sem apoio estrangeiro na operação das redes contra terrorismo ou contra crimes cibernéticos (SUL21, 2012).

> A missão de proteger os ativos de órgãos governamentais no espaço cibernético durante os Grandes Eventos foi atribuída, pelo Ministério da Defesa, ao Exército Brasileiro, que criou um eixo de atuação específico chamado Defesa Cibernética. A complexidade e a importância da missão levaram à evolução da estrutura organizacional existente no Exército, culminando com a criação, em outubro de 2014, do Comando de Defesa Cibernética (BRASIL, 2018a, p.111).

O evento foi um teste para a nascente estrutura de defesa cibernética do país, o CDCiber. O Centro de Defesa Cibernética foi um precursor e pioneiro no tema, já que o Brasil sediaria também a Copa do Mundo e os Jogos Olímpicos. Na ocasião foi instalada uma “sala de crise” que permitiu verificar em tempo real o que estava ocorrendo na Rio +20 em termos de monitoramento de rede (SÁ, 2012).

Em agosto de 2011 foi criada a Secretaria Extraordinária de Segurança para Grandes Eventos (SESGE) por meio do Decreto nº 7.538 – SG/PR e integrada ao Ministério da Justiça (MJ) e chefiada por delegados da Polícia Federal (BRASIL, 2011). Esse normativo seria alterado posteriormente, em 2012, por meio do Decreto nº 7.682, que viria a alterar o rol de grandes eventos abrangidos pelas competências da SESGE e definir a sua data de extinção para julho de 2017 (BRASIL, 2012).

Foi estabelecida com o objetivo de planejar as ações de Segurança Pública e

Defesa Civil para a Copa do Mundo, Olimpíadas e Paraolimpíadas – além de outros eventos internacionais, como a Jornada Mundial da Juventude e a Copa das Confederações (ADPF, 2018).

> § 1º Para os fins do disposto neste Decreto, consideram-se grandes eventos:
> I - a Jornada Mundial da Juventude de 2013;
> II - a Copa das Confederações FIFA de 2013;
> III - Copa do Mundo FIFA de 2014;
> IV - os Jogos Olímpicos e Paraolímpicos de 2016;
> V - outros eventos designados pelo Presidente da República.
> § 2º A Secretaria Extraordinária de Segurança para Grandes Eventos será extinta em 31 de julho de 2017 (BRASIL, 2012).

"Como consequência, o planejamento e a execução da segurança durante as Copas e os Jogos Olímpicos adquiriram uma nova dimensão, passando a ocorrer de maneira integrada pelo Ministério da Justiça (MJ) e Ministério da Defesa (MD)" (BRASIL, 2018a, p.7).

As ações foram divididas em três segmentos: DEFESA, SEGURANÇA e INTELIGÊNCIA. O Ministério da Defesa era responsável por todas as ações das Forças Armadas, coordenadas pelo MD. A Segurança compreendia todas as ações dos órgãos de segurança pública (OSP) coordenadas pelo MJ e Secretarias de Segurança Pública dos estados. O segmento de Inteligência compreendia as ações dos órgãos do Sistema Brasileiro de Inteligência, coordenadas pela Agência Brasileira de Inteligência (ABIN) (BRASIL, 2018a, p.11 - 12). A figura 26 apresenta as ações previstas para a Segurança e a Defesa.

Figura 26 - Áreas de interesse de segurança

Fonte: (BRASIL, 2018a, p.12)

Logo após a Conferência Rio +20, o Governo Federal emitiu os primeiros documentos esboçando o modo de governança da segurança nos Grandes Eventos. Um Comitê Executivo de Segurança Integrada (CESI – figura 27) foi criado e subordinado à Presidência da República.

O CESI era constituído pelo Chefe da Casa Civil da Presidência da República (CCPR), na função de coordenador, Ministro da Justiça e pelo Ministro da Defesa. O grupo tinha como seus elementos de coordenação e controle das ações o Estado-Maior Conjunto das Forças Armadas, a Secretaria Especial de Segurança para Grandes Eventos e a Agência Brasileira de Inteligência (BRASIL, 2018a, p.13).

Figura 27 - Comitê Executivo de Segurança Integrada - CESI

Fonte: (BRASIL, 2018a, p. 13)

3.2. Copa das Confederações (2013)

O primeiro torneio foi realizado na Arábia Saudita no ano de 1992 com quatro equipes, seguida de duas novas edições no ano de 1995 e 1997 no mesmo país, a qual primeiramente era conhecida como Copa Rei Fahd ou ainda Torneio Intercontinental, e a partir de 1997 ficou conhecida como Copa FIFA das Confederações (BONFIM, 2013, p.89).

O campeonato era organizado pela Federação Internacional de Futebol (FIFA), entre as seleções nacionais a cada quatro anos e serviu como preparação para o país-sede da Copa do Mundo e para as seleções que iriam lutar pelo título mundial (STROZI, 2013). A última competição aconteceu em 2017, com a vitória alemã sobre o Chile. Atualmente a FIFA decidiu não realizar mais a Copa das Confederações, a fim de expandir a Copa do Mundo de Clubes (BURTON, 2022).

A nona edição da Copa das Confederações (sétima edição da Copa das Confederações organizada pela FIFA) foi realizada entre 15 a 30 de junho de 2013 em diferentes cidades do Brasil: Belo Horizonte, Brasília, Fortaleza, Recife, Rio de Janeiro e Salvador. O torneio foi preparatório para a Copa do Mundo de 2014, que ainda seria realizado no país.

A Copa das Confederações foi também um período de intensas manifestações políticas nas principais cidades brasileiras. Segundo Romão (2013, p. 11) entende-se que as manifestações tiveram caráter episódico, movidas por uma conjuntura que agregou pelo menos quatro fatores preponderantes:

1. a existência de um movimento organizado que impulsionou as primeiras manifestações com uma demanda objetiva, o Movimento Passe Livre (MPL);
2. a descabida repressão policial que, a certa altura dos acontecimentos, alterou o posicionamento da grande mídia a favor dos manifestantes;
3. a concomitância de um evento esportivo de âmbito mundial que funcionou, ao mesmo tempo, como combustível e veículo da ocorrência das manifestações; e
4. o contexto de descontentamento generalizado com o sistema político.

> O MPL talvez seja o primeiro grande movimento social pós-Lula, pós-hegemonia do Partido dos Trabalhadores (PT), no campo da esquerda no país. O MPL não é filiado a nenhuma central de movimentos ou central sindical. Suas lideranças não têm raízes no movimento social que ajudou a combater a ditadura militar, que participou da Constituinte, que lutou no Fora Collor ou que resistiu às privatizações no governo Fernando Henrique Cardoso (FHC). Embora tenha militantes ligados a partidos políticos de esquerda, sua forma de organização está muito mais próxima das tradições do anarquismo libertário, que pressupõe horizontalidade nas decisões e aversão a espaços de negociação com o Estado. É filha de Seattle e Gênova. No entanto, não se exime de acolher indivíduos militantes filiados a partidos políticos no movimento. São apartidários, mas não antipartidários (ROMÃO, 2013, p.11)

Para Romão (2013, p. 13), provavelmente, o único tema unificador das demandas foi a repulsa à Copa do Mundo (e das Confederações) e à presença da FIFA no país, pois a base organizada dos protestos era oposta aos gastos excessivos na construção dos estádios de futebol, chamados de “arenas”. Existia uma impressão observada na cultura política dos protestos de uma subserviência excessiva do governo brasileiro aos ditames da Fifa.

> O fato de a própria Fifa estar longe de ter dirigentes de conduta ética ilibada, o que aflora ainda mais um sentimento anticorrupção que se conecta no imaginário coletivo à repulsa

> aos chamados “mensaleiros” e à geleia geral das alianças entre os partidos políticos (mais considerações sobre esse tema serão apresentadas a seguir); a conexão direta entre um país moldado “para inglês ver” – o país da Copa – e o Brasil real, que requer mais e melhores hospitais e escolas. A exigência bem-humorada e espontânea de hospitais e escolas “padrão Fifa” certamente será uma das marcas dos protestos ocorridos em junho. O tema da repulsa à Fifa traz também outro componente ímpar com relação às manifestações de junho: o sentimento nacionalista. O Hino Nacional cantado nas ruas e repetido pelas torcidas nos jogos da Seleção Brasileira ressoa um sentimento de um país que, apesar de sua classe política, tem orgulho de si mesmo, de sua atual posição no concerto das nações e, naquele contexto, de ter rompido um estado de passividade e letargia com relação aos assuntos públicos e da política. Nunca no Brasil o dístico fascista “meu partido é meu país” foi tão repetido. Nesse sentido, os grupos de extrema-direita relativamente organizados obtiveram pico na sua capacidade de liderar parcelas dos cidadãos que – embora sejam contra a violência e o saque – estão de acordo com relação ao princípio de que os partidos políticos são o mal a ser combatido (ROMÃO, 2013, p.11 - 12).

“Essas manifestações foram marcadas por diversos atos de violência e vandalismo, pela quase “espontaneidade” e pelo grande número de manifestantes em cada um dos atos” (BRASIL, 2018a, p.21). Esses movimentos sociais foram caracterizados com o funcionamento em rede e o ciberativismo pelos grupos centralizadores dos protestos de junho e organizados por páginas eletrônicas e que se mantiveram presentes nas manifestações nos meses decorrentes, a saber: *Anonymous* e os *Black Blocs* (COSTA; CARDOSO; MEDINA, 2013, p.01).

> O grupo *Anonymous* é composto por uma rede internacional, minimamente organizada de hacktivistas, que teve sua raiz nos quadro de avisos baseado em imagens do website “4chan”. O site começou em 2003 e é usado por pessoas em todo o mundo. O título enfatiza o desejo do grupo de usar os conhecimentos tecnológicos para um propósito e causa específicos. “Hacktivista” é uma fusão entre “hacker” e “ativista”. Quando as pessoas têm habilidades técnicas, acesso à Internet e entendem como a infraestrutura de rede e os servidores funcionam, pode ser útil colocar esse conhecimento para ter algum efeito no mundo. Eles não fazem *hacking* e *cracking* sem uma causa. A crença do “corpo de membros” sobre a função do *Anonymous* em todo o mundo é: as corporações e organizações que são consideradas corruptas ou danosas à liberdade devem ser atacadas. Se por algum motivo o administrador de uma rede acredita que pode se tornar um alvo, é melhor testá-la para lidar com ataques DDoS, pois é o método mais comum que o *Anonymous* usa para derrubar servidores da web (KOVACS, 2023).

> *Black blocs* é composto por pequenos grupos de afinidade, muitas vezes organizados no próprio momento da manifestação, os quais atuam de forma independente dentro destas (TAKAHASHI, 2013). Não seria exatamente uma organização, mas uma ideia, uma tática de autodefesa contra a violência policial, além de forma de protesto estético baseada na depredação de símbolos do estado e do capitalismo. A dinâmica *black bloc* remete a uma rede descentralizada ao invés de um movimento orgânico e coeso (COSTA; CARDOSO; MEDINA, 2013, p.10 - 11)

Esse ciberativismo, ou ativismo digital, revolucionou o modo como os movimentos sociais se organizam e transmitem suas mensagens ao resto da sociedade. Um simples clamor nas redes sociais pode reunir um grupo considerável de pessoas para a realização de ações políticas e coletivas, como protestos, boicotes, ocupações e marchas.

O ciberativismo tornou-se uma ferramenta valiosa para a contemplação das demandas sociais e para a mobilização de pessoas, o que pode ser realizado em um curto espaço de tempo. O aumento do acesso às informações por meio de dispositivos eletrônicos, como celulares, notebooks, redes sociais, facilita o contato entre milhões de pessoas de todo o mundo, que se comunicam instantemente. Por isso, os movimentos sociais ganham o reforço necessário para disseminação de propostas, eventos, assuntos e estratégias que trafegam em um público cada vez maior. Não há fronteiras físicas e nem digitais cujo acesso aos ideais dos movimentos não sejam quebradas pelo ciberativismo (COSTA; CARDOSO; MEDINA, 2013, p.07).

> Paralelamente, o uso dos meios digitais pelos movimentos sociais tem causado uma mudança na organização destes. Se antes um movimento social era composto por pessoas que estavam geograficamente próximas e usualmente dirigidas verticalmente, atualmente consta-se uma horizontalidade na forma como os movimentos sociais se associam e uma descentralização na sua organização. A possibilidade de as pessoas entrarem no mundo cibernético rompe com os modelos alicerçados em volta de um líder ou uma figura que oriente o movimento (COSTA; CARDOSO; MEDINA, 2013, p.07 - 08).

Sandor Vegh (2003) apresenta uma classificação do ciberativismo de acordo com seus objetivos e funções. O primeiro objetivo diz respeito à conscientização e à argumentação, o segundo envolve organização e mobilização e o terceiro, ação e reação.

Em relação ao objetivo 1 - conscientização e argumentação - trata-se da defesa de determinadas causas que são relevantes para o público de forma geral e que extrapolam o domínio e controle das mídias tradicionais, por isso o uso da Internet como uma forma alternativa para divulgação de informações por indivíduos e/ou organizações independentes. As formas de divulgação dessas informações podem ser via redes sociais, *websites* ou uma lista de distribuição de e-mails. A disseminação de informações contribui para formar uma rede de pessoas que podem ser organizadas e mobilizadas para determinados propósitos.

Quanto ao objetivo 2 - organização e mobilização – a internet pode ser utilizada de três formas distintas: a primeira forma é usada para acionar as pessoas por meio de ações *off-line.* Neste caso uma manifestação pode ser convocada via publicações em sites ou por envio de e-mails, onde é inserido o local e o horário do evento. A segunda forma pode ser considerada um híbrido, pode-se utilizar uma ação *off-line*, mas é mais eficiente se for *online.* No caso, o uso de e-mails caracterizando uma ação *off-line*, mas com o objetivo, por exemplo, de um contato direto com um representante político via correio eletrônico, ou seja, uma ação *online*. Neste caso específico, Vegh menciona que não saberia avaliar qual o melhor impacto, o envio de uma grande quantidade de e-mails ou

de mensagens encaminhadas via cartas manuscritas. A terceira forma, o uso de um apelo direto para uma ação online, como por exemplo, o uso de campanhas massivas de envio de *SPAM* ou de mensagens eletrônicas com objetivo de sobrecarregar o serviço de e-mail de um alvo específico.

Por último, o objetivo 3 - ação e reação – ocorre quando os ataques *online* são praticados por grupos de *hackers*, que podem ser motivados por questões políticas ou financeiras. Para fins de exemplo, o uso de ataques de DDoS com a finalidade de sobrecarregar as páginas da *Web* para indisponibilizá-las na Internet. Neste caso, busca-se chamar atenção para um evento ou para uma causa em particular. A ideia é fazer do "hacktivismo" uma forma de usar a tecnologia e as mídias eletrônicas para avançar nas conquistas de direitos humanos.

> A possibilidade de comunicação rápida, barata e de grande alcance faz atualmente da Internet o principal instrumento de articulação e comunicação das organizações da sociedade civil, movimentos sociais e grupos de cidadãos. A rede se tornou um instrumento útil e eficaz para as demandas sociais em um espaço público fundamental (MACHADO, 2007, p. 268).

O seu poder de aglutinar dezenas ou até centenas de organizações de diferentes contextos socioeconômicos, culturais, identitários e linguísticos faz com que o descontentamento, sejam quais forem os motivos, torne-se um agregador de sinergias amplas e complexas de ações globais. É a formação de um novo caminho para interação política, cultural, social e econômica, pois uma pessoa de qualquer lugar do mundo pode assumir diferentes tipos de papeis simultaneamente, como cidadão, militante, editor, distribuidor, consumidor, articulador, etc, independe das fronteiras geográficas e da interferência direta de governos e corporações (MACHADO, 2007, p. 268–269).

Além de todo esse contexto de conflitos sociais e políticos durante o período da Copa das Confederações, o governo brasileiro precisou lidar também com o vazamento de informações disponibilizados por Edward Snowden, ex-técnico da CIA (*Central Intelligence Agency*). Pois além de espionar a população americana, vários países da Europa e da América Latina foram alvos da ação, entre eles o Brasil. Snowden demonstrou por meio de documentos vazados que o governo americano, mais especificamente a NSA (*National Security Agency*), monitorava conversas de e-mail da presidente Dilma Rousseff. Nesse caso, o Brasil ficou atrás apenas dos Estados Unidos em volume de monitoramento e interceptações. A presidente Dilma e seus assessores foram alvos específicos e diretos de espionagem (MARTINS, 2016, p.06).

> A segurança cibernética da NSA previne e erradica ameaças aos sistemas de segurança nacional dos EUA, com foco na defesa do setor industrial e na melhoria da segurança do armamento dos EUA. Também atua para promover a educação, a pesquisa e a construção de carreira em segurança cibernética. A NSA é responsável por fornecer informações advindas da inteligência de sinais de outras nações aos legisladores e às forças militares americanas. A SIGINT (*Signals Intelligence*) desempenha um papel vital na segurança nacional, fornecendo à liderança norte-americana informações críticas de que necessitam para defender o país, salvar vidas e promover os objetivos e alianças dos EUA a nível global (ESTADOS UNIDOS, 2024).

Essas denúncias repercutiram no meio político brasileiro e tiveram ampla cobertura jornalística. Esperava-se que o governo brasileiro reagisse de forma enérgica e cobrasse do governo norte-americano explicações sobre a espionagem descoberta. Uma das atitudes tomadas pelo Brasil para demonstrar a sua insatisfação foi cancelar uma missão brasileira aos Estados Unidos e iniciar uma investigação interna sobre o vazamento da espionagem governamental dos EUA (MARTINS, 2016, p. 6) .

O Ministério da Defesa e as Forças Armadas fizeram uma varredura para tentar encontrar indícios de invasão nos sistemas criptografados que armazenavam informações sensíveis e estratégicas do governo brasileiro, mas não identificaram nenhuma quebra de segurança da informação. Mesmo assim, o Congresso Nacional decidiu pela abertura de uma Comissão Parlamentar de Inquérito (CPI), em 10 de agosto de 2013, conhecida como CPI da Espionagem para investigar o suposto monitoramento em massa. A sua duração foi de 7 meses e contou com a participação de 13 senadores entre titulares e suplentes (MARTINS, 2016, p. 6).

O relatório final da CPI não conseguiu determinar se houve espionagem nos moldes das revelações apresentadas por Snowden, mas que havia indícios factíveis de o governo brasileiro ter sido espionado pelos EUA. A CPI concluiu que a questão mais importante era a adoção de medidas práticas para estancar as vulnerabilidades na segurança cibernética brasileira e a implementação de transparência e controle sobre as requisições de dados solicitadas em território nacional. O relatório final também recomendou as seguintes ações (MARTINS, 2016, p. 6–7):

- Um maior investimento na área de inteligência e contrainteligência por conta da vulnerabilidade observada atualmente na área;
- Investimentos em tecnologia própria e nacional;
- Capacitação de profissionais para atuação na área;
- A publicação do Plano Nacional de Inteligência pela Presidência da República;
- A criação de uma Agência Brasileira de Inteligência de Sinais, para operar no ambiente virtual e que tenha um caráter ofensivo;
- A aprovação da PEC nº 67, de 2012, que eleva a atividade de inteligência ao nível constitucional, cria um sistema de brasileiro de inteligência com fiscalização do Poder Legislativo (MARTINS, 2016, p. 7).

Toda essa conjuntura social e de espionagem resultou em medidas para o fortalecimento da segurança cibernética brasileira e para o debate sobre a guerra cibernética.

3.3. Jornada Mundial da Juventude (2013)

O Brasil sediou entre os dias 23 e 28 de julho a Jornada Mundial da Juventude (JMJ), considerado um evento religioso da Igreja Católica, que reúne milhões de jovens desde 1987. O país nesse período recebeu a presença do Papa Francisco que participou de atividades programadas nas cidades do Rio de Janeiro – RJ e Aparecida do Norte (SP).

O Ministério da Defesa fez-se presente no evento por meio da coordenação do Estado-Maior Conjunto das Forças Armadas (EMCFA) para planejamento e na execução de atividades relacionadas à segurança da JMJ. Realizou trabalho integrado com o Ministério da Justiça e órgãos de segurança pública nos níveis federal, estadual e municipal. Atuou em dez setores estratégicos de defesa do Estado: o de Defesa Aeroespacial e Controle do Espaço Aéreo; Defesa de Áreas Marítimas e Fluviais; Defesa de Estruturas Estratégicas; Emprego de helicópteros; Prevenção ao Terrorismo; Preparo e Emprego de Força de Contingência; Fiscalização de Explosivos; Segurança e Defesa Cibernética; Defesa Química, Biológica, Radiológica e Nuclear; além da cooperação na segurança de chefes de Estado, na Defesa Civil e na proteção das fronteiras (BRASIL, 2022a).

No Palácio Duque de Caxias, no Centro do Rio, sede do Comando Militar do Leste (CML), funcionaram os centros de Coordenação Tático Integrado, de Defesa Área, e de Defesa Cibernética (SOUZA; GONÇALVES, 2013). O Centro de Defesa Cibernética (CDCiber) também monitorou as redes sociais para aumentar a segurança dos eventos com a vinda do Papa Francisco, da mesma forma como ocorreu durante a Rio +20 e a Copa das Confederações da Fifa. As forças militares utilizaram um software comprado da empresa catarinense Dígitro[30]. Segundo o general José Carlos dos Santos, militar à

[30] Pelo site da empresa Dígitro (https://www.digitro.com/quemsomos) é possível visualizar um vídeo na plataforma Youtube de 4 minutos e vinte e cinco segundos (https://www.youtube.com/watch?v=GnbFUKWE66E) , que apresenta o programa Guardião Online, uma ferramenta que possibilita a análise eficiente de grandes volumes de dados gerados a partir de serviços em nuvem, possibilitando mais eficiência para as investigações e mais segurança para a gestão de dados, por otimizar os processos de coleta, armazenamento e processamento das informações com segurança e controle da cadeia de custódia. Ao final do vídeo, a Dígrito se autodenomina uma empresa estratégica de defesa, certificada pelo Ministério da Defesa do Brasil.

frente do Centro, o programa fazia uso de filtros de grupos de palavras e expressões para destacar informações de interesse para a segurança pública (ROCHA, 2013).

Sites como Facebook, principal deles, e o Twitter, responderam por 5% das mensagens analisadas. As informações eram colhidas de fontes abertas, sem contato direto com as empresas prestadores de serviços nessa área, nenhum contato com servidores de e-mail ou com companhias telefônicas, conforme informado pelo general Santos. As informações eram captadas e repassadas para os órgãos de segurança pública e a departamentos do próprio Exército. Segundo Santos, as informações repassadas se tratavam de instruções de como fazer coquetéis molotov, como usar bolinhas de gude para dificultar a atuação da cavalaria de policiais militares e orientação do uso de máscara contra gás lacrimogênio e gás de pimenta (GOMES, 2013).

Em relação ao ciberterrorismo não foram identificadas ameaças reais, apenas suposições, descartadas pela inteligência do Exército, mas por conta das informações levantadas pelas ferramentas de inteligência cibernética nas mídias sociais, algumas fábricas clandestinas de material explosivo no Nordeste foram fechadas e algumas pessoas foram presas (GOMES, 2013).

Santos destacou que o monitoramento de mídias sociais recebeu como atribuição temporária para o JMJ, que o cerne do trabalho estava mais voltado para ameaça cibernética, quanto a possibilidade de ataque às redes de dados brasileiras, entre os grupos no radar estava o grupo *Anonymous*, pois estava tentando corromper redes envolvidas com eventos, por meio de ataques de negação de serviço (GOMES, 2013).

3.4. Copa do Mundo (2014)

O Brasil foi escolhido pela FIFA em 2009 para sediar a Copa do Mundo em 2014; o evento mobilizou o país e a comunidade internacional, sendo que efetivamente transcorreu no período de 12 de junho a 13 de julho de 2014. Além da seleção brasileira de futebol, 31 seleções competiram entre si em 12 diferentes cidades-sedes: Belo Horizonte (MG), Brasília (DF), Cuiabá (MT), Curitiba (PR), Fortaleza (CE), Manaus (AM), Natal (RN), Porto Alegre (RS), Recife (PE), Rio de Janeiro (RJ), Salvador (BA) e São Paulo (SP). Diferente da Copa das Confederações, a Copa do Mundo teve a inclusão de 5 cidades-sede: Cuiabá, Curitiba, Natal, Porto Alegre e São Paulo (RODRIGUES, 2018, p.56).

Um pouco antes da Copa começar, o governo brasileiro, segundo uma reportagem

da rádio de notícias CBN (2014), havia identificado os principais grupos de *hackers* que ameaçavam ataques cibernéticos durante a Copa do Mundo e lançou um contra-ataque cibernético para evitar ação de *hackers* no período do evento. Empresas de tecnologia da informação responsáveis pelos portais públicos prepararam um esquema de plantão especial durante o período da Copa e com apoio de grupo de contrainteligência e contra-ataque, realizaram monitoramento em diversos sites, principalmente nas redes sociais. O esquema de segurança cibernética funcionava 24 horas todos os dias da semana. As equipes de plantão trabalhavam de forma multidisciplinar, envolvendo especialistas em banco de dados, rede e segurança. O trabalho era feito em parceria com a Polícia Federal, que era acionada quando a ameaça ou o ataque era identificado.

O Serpro - Serviço Federal de Processamento de Dados, que é responsável por várias plataformas do Governo na Internet, incluindo, por exemplo, a Presidência da República, o Ministério da Fazenda, a Receita Federal, admitiu que no período de Copa do Mundo existiu uma preocupação especial com o aumento de fluxo de rede e com as ameaças dos *hackers*. E ressaltou que não havia esquema de segurança 100% na rede, que era preciso sempre ficar em alerta e que não existia nem dia e nem horário. Trabalhar com segurança da informação era como uma Unidade de Tratamento Intensivo (UTI), a qualquer momento poderia ser acionado e por isso a equipe precisaria estar de prontidão. O SERPRO manteve uma parceria muito boa com a Polícia Federal para tratar dessas questões (CBN, 2014).

Mesmo assim, *hackers* conseguiram invadir a página do Comitê Paulista da Copa do Mundo e do Tribunal de Justiça do Distrito Federal. No período da Copa das Confederações chegaram a divulgar dados de Policiais Militares nos Estados (CBN, 2014).

Durante a Copa do Mundo de 2014, a Arcon Labs (NEC), uma empresa provedora de soluções integradas de Tecnologia da Informação e Comunicação, registrou um aumento de 57% nos ataques relacionados à segurança da informação (NEC, 2018).

Enquanto isso integrantes da equipe de inteligência da Polícia Federal identificaram grupos na Internet que pretendiam realizar um grande número de invasões e promover congestionamentos em sistemas e sites ligados ao governo no dia de abertura da Copa do Mundo, 12 de junho. Uma semana antes do início da Copa, o Itamaraty foi alvo de ataques cibernéticos, a PF ainda descobriu que alguns dos usuários de e-mails capturados por *hackers* foram usados para a realização de protestos contra a Copa do Mundo. Uma mensagem contrária à realização do mundial no Brasil chegou a ser postado

na página de intranet do ministério. As investigações apontaram que pessoas ligadas ao grupo *Anonymous* no Brasil participaram dos ataques (NERY, 2014).

Um ano antes do início da Copa, o grupo *Anonymous* já havia realizado um ataque cibernético que tirou do ar o portal do governo federal sobre o Mundial. O site copa2014.gov.br, administrado pelo Ministério do Esporte, ficou inacessível por um tempo. O site disponibilizava informações sobre investimentos para a realização do torneio e também da Copa das Confederações (KONCHINSKI, 2013).

Meses antes do início do Campeonato Mundial, uma matéria jornalística do G1 reportou uma entrevista da empresa de notícias Reuters com um participante do grupo *Anonymous* que prometia diversos ataques contra os sites vinculados à Copa. A ideia era encontrar vulnerabilidades para quebrar a segurança cibernética brasileira para promover invasões, pois a Copa oferecia uma audiência internacional muito grande e que seria aproveitada para mostrar a indignação dos grupos em relação ao Mundial no Brasil. O *Anonymous* estava descontente com a realização da Copa do Mundo principalmente devido às altas quantias de dinheiro que foram gastas para a realização do torneio. Uma das estratégias para demonstrar essa insatisfação era fazer uso de ataques DDoS para indisponibilizar sites governamentais e de parceiros da FIFA (G1, 2014).

Segundo Schiavi (2014), o grupo de hackers *Anonymous* cumpriu com a promessa de realizar uma série de ataques cibernéticos durante a Copa do Mundo para atrapalhar o andamento do evento, entre os sites atacados estavam o Sistema Brasileiro de Inteligência (SISBIN), que reúne órgãos federais para a troca de informações e conhecimentos de Inteligência, como também os sites da Hyundai Brasil, Confederação Brasileira de Futebol, Departamento de Justiça, Polícia Militar de São Paulo, Banco do Brasil e Africa.com.br, todos com negação de serviço distribuída (DDoS). O grupo realizou testes para identificar quais sites estavam mais vulneráveis, o plano de ataque estava também voltado para os patrocinadores da Copa do Mundo (SCHIAVI, 2014).

Na época o Chefe do Estado Maior da coordenação de defesa de área (CMA), coronel Henrique Batista, destacou que o alvo principal dos *hackers* eram as estruturas de comunicações públicas e privadas, sistemas de controle crítico (energia elétrica e nuclear e segurança pública), além do furto de informações de caráter reservado de órgãos e instituições privadas. Os golpistas para conseguirem informações privadas utilizavam a criatividade para atacar fãs do futebol enviando conteúdos contaminados por e-mail e redes sociais. Empresas especializadas em segurança da informação identificaram diversas ações de *hackers* que atuavam dessa forma. O tipo de ataque mais comum era

ofertar supostos ingressos gratuitos via e-mail para assistir às partidas da Copa, pois sabiam que esse era o desejo de qualquer apaixonado por futebol (FAN, 2014).

De acordo com Batista, o Governo Federal, em sua preparação para a Copa do Mundo, efetuou análise de risco em serviços e instalações para minimizar as vulnerabilidades cibernéticas e aprimorar a segurança da informação e comunicação. Em todas as áreas críticas foram disponibilizadas equipes capacitada para identificar e tratar ameaças cibernéticas, um trabalho que envolveu instituições como o Gabinete de Segurança Institucional e o Ministério de Defesa Cibernética (FAN, 2014).

3.5. Jogos Olímpicos e Paraolímpicos (2016)

Os jogos gregos e os Jogos Olímpicos estavam atrelados a um dos rituais religiosos da Grécia Antiga. Pode-se considerar um festival que homenageava o deus Zeus. Os jogos eram realizados na cidade de Olímpia e o primeiro campeão olímpico listado nos registros foi Coroebus de Elis, um cozinheiro, que venceu a corrida de velocidade em 776 a.C (YOUNG; ABRAHAMS, 2024).

> Os Jogos Olímpicos foram tecnicamente restritos aos gregos nascidos livres. Muitos concorrentes gregos vieram das colônias gregas na península italiana e na Ásia Menor e na África. A maioria dos participantes eram profissionais que treinavam em tempo integral para os eventos. Esses atletas ganharam prêmios substanciais por vencerem muitos outros festivais preliminares e, embora o único prêmio em Olímpia fosse uma coroa de flores ou guirlanda, um campeão olímpico também recebia adulação generalizada e, muitas vezes, benefícios generosos de sua cidade natal (YOUNG; ABRAHAMS, 2024).

A Grécia sempre considerou que havia uma ligação estreita e de direito com os Jogos Olímpicos, pois foi o local onde nasceram as primeiras competições esportivas. O resto do mundo também reconheceu a prerrogativa da Grécia de se considerar o berço dos Jogos e de agir como guardiã através dos tempos do espírito olímpico e como a fonte produtora da ideologia olímpica. Portanto, para a Grécia foi de grande importância simbólica AO sediar os Jogos Olímpicos de 1896 e 2004 (SKLAVENITIS, 2006, p.7-8).

As ideias e o trabalho de diversas pessoas levaram à criação das Olimpíadas modernas. Segundo Young (2004, p.156-157) os jogos modernos não têm apenas um fundador; pelo menos cinco homens foram indispensáveis: um francês, um inglês e três gregos, são, nomeadamente, Pierre Coubertin, Brookes, Soutsos, Zappas e Vikelas. O arquiteto mais conhecido dos Jogos modernos foi Pierre, barão de Coubertin, nascido em Paris no dia de Ano Novo de 1863 (YOUNG; ABRAHAMS, 2024). Pode se dizer que

ele lançou os princípios para a restauração do Jogos: celebração de quatro em quatro anos como na Antiguidade; modernização do programa esportivo; rotatividade dos Jogos entre as principais cidades do mundo e a criação do Comitê Olímpico Internacional - COI (COLLI, 2004, p.11).

Em relação aos jogos paralímpicos, em 1944, o Reino Unido estabeleceu um hospital para tratamento dos soldados feridos na Segunda Guerra Mundial, dedicado a soldados com lesões medulares, localizado em Stoke Mandeville. A instituição ficou conhecida como *Spinal Injuries Centre* ou Hospital de Lesionados Medulares, na tradução para o português.

Em 1948, enquanto aconteciam os Jogos Olímpicos de Verão em Londres, o neurologista alemão Ludwig Guttmann, que utilizava o esporte na reabilitação física, promoveu os Jogos do *Stoke Mandeville*, envolvendo os pacientes do hospital de mesmo nome, em sua maioria veteranos da Segunda Guerra Mundial. A primeira competição internacional para pessoas com deficiência ocorreu quatro anos depois nas Olimpíadas de Helsinki (Finlândia), quando uma delegação dos Países Baixos viajou para Londres para disputar os Jogos do *Stoke Mandeville* (SOBREIRA, 2021).

> A partir de 1960, em Roma (Itália), o evento esportivo passou a ser realizado na mesma sede dos Jogos Olímpicos. Ainda chamada de "Olimpíadas dos Portadores de Deficiência", essa é considerada a primeira Paraolimpíada da história, com delegações de 23 países, um total de 400 atletas, todos com lesão na medula espinhal. Mesmo sem ser abraçada de imediato pelo Comitê Olímpico Internacional (COI), a competição passou a ser realizada a cada quatro anos, sempre nas semanas posteriores aos Jogos Olímpicos de Verão (SOBREIRA, 2021).

Inicialmente a competição era restrita a pessoas com lesão na medula espinhal, mas foi gradualmente ampliada para pessoas com outras deficiências. O Brasil não teve delegação em Roma (1960), mas somente em 1984, quando o termo Jogos Paraolímpicos passou a ser usado e ampliou-se a participação com atletas com paralisia cerebral, o país conquistou 28 medalhas, ficando na classificação geral em 24º lugar (SOBREIRA, 2021).

Em outubro de 2009, o Rio de Janeiro foi eleito sede dos Jogos Olímpicos e Paraolímpicos de 2016. Foi a primeira vez que o maior evento multiesportivo do mundo aconteceu na América do Sul, após o Rio vencer a disputa com as cidades de Madri, Chicago e Tóquio (GLOBO, 2021).

Apesar de não ter tido apoio unânime, a candidatura do Rio de Janeiro à sede olímpica mobilizou o país inteiro, com engajamento dos governos federal, estadual e municipal. A aprovação de leis específicas, o uso de recursos públicos para a viabilização dos jogos e a garantia de benefícios para a população colocaram o Congresso Nacional

na órbita das Olimpíadas (OLIVEIRA, 2015).

A abertura oficial foi no Maracanã no dia 5 de agosto de 2016, assim como o encerramento, no dia 21 de agosto. Segundo o Comitê Olímpico Brasileiro (COB), o Brasil participou com 465 atletas, sendo 256 homens e 209 mulheres. Os Jogos Olímpicos Rio 2016 contaram com a maior delegação brasileira na história da competição. As equipes esportivas brasileiras finalizaram sua participação com o recorde à época de 19 medalhas, a inédita 12ª colocação no quadro geral de medalhas (empatado com a Holanda) e o maior número de ouros (COB, 2016).

Em relação aos Jogos Paraolímpicos, a abertura ocorreu no dia 07 de setembro de 2016 no estádio do Maracanã. A Cerimônia de Encerramento, que ocorreu no dia 18 de setembro, encerrou um ciclo de megaeventos sediados no Brasil, que recebeu a Copa das Confederações 2013, a Copa do Mundo 2014 e as Olimpíadas antes de sediar as Paraolimpíadas (BRASIL, 2016).

O Comitê Paraolímpico Internacional (IPC, em inglês) informou que os Jogos Paraolímpicos Rio 2016 foram os mais vistos da história, com uma audiência acumulada de mais de 4,1 bilhões de pessoas.

> Um total de 154 nações transmitiram os jogos, 39 a mais do que Londres 2012 e quase o dobro dos 80 que haviam mostrado Pequim 2008. Como consequência, cerca de 5.110 horas de eventos esportivos foram mostradas, mais do que Pequim e Londres combinados. Além do recorde de transmissões de TV em plataformas convencionais, mais de um bilhão de pessoas interagiram com os jogos por meio dos canais de mídia digital (CPB, 2017).

Vale ressaltar que a cerimônia de abertura dos Jogos do Rio de Janeiro foi muito elogiada pela mídia de todo o mundo, destacando-se inclusive o fato de que ela custou apenas 10% da última edição olímpica ocorrida em Londres. No entanto, a criatividade e o jeitinho brasileiro deram um jeito de encobrir um rombo no orçamento ocorrido pouco meses antes do início dos jogos, o que levou à necessária improvisação por parte dos idealizadores da abertura. O Brasil passava por uma grave crise institucional, manifestada por uma onda de protestos (RUBIO, 2018, p. 98).

No dia 05 de agosto, horas antes da cerimônia de abertura dos Jogos Olímpicos do Rio, o grupo *Anonymous* publicara na conta Anonymous Brasil da conta do Facebook uma mensagem com o título “Olá, Rio de Janeiro”. Em meio aos protestos com os gastos públicos para a realização do evento, o grupo começou a atacar os sites do governo brasileiro por ocultar por trás da grandiosidade da Olímpiada, a pobreza generalizada na cidade, as expropriações agressivas, a violência policial e a repressão a manifestantes.

Por causa disso, o grupo lançou diversos ataques de negação de serviço (DDoS) contra sites dos governos estadual e municipal, logo após a declaração do grupo nas redes sociais. Foram derrubados pelo menos cinco sites, entre eles: www.brasil2016.gov.br, www.rio2016.com, www.esporte.gov.br, www.cob.org.br e www.rj.gov.br (MUGGAH; THOMPSON, 2016).

No dia 08 de agosto, seis sites foram indisponibilizadas, o da Polícia Militar fluminense, do Instituto de Segurança Pública do Estado do Rio, da Companhia Municipal de Limpeza Urbana (COMLURB) e do Programa Internet Comunitária. Todos os próximos alvos eram divulgados pelo *Anonymous* (MUGGAH; THOMPSON, 2016).

Segundo apurou Rohr e Gomes (2016) com a empresa de Segurança Symantec, as Olímpiadas e Paraolimpíadas de 2016 tiveram em média 2,7 incidentes cibernéticos por hora. Foram 2.686 incidentes durante os 41 dias de duração dos dois eventos. Para cada "incidente" entende-se um conjunto de eventos ou ataques relacionados, que necessitaram de intervenção de especialistas da empresa. Do total de ocorrências, 24 foram classificadas como "críticas" ou "emergenciais". Destaca-se entre os incidentes mais graves, o ataque de "*spear phishing*". Como exemplo, a Symantec citou o caso da mensagem enviada e direcionada para um alto executivo da Rio 2016 com a intenção de roubo de informações.

> O que torna os golpes de *spear phishing* tão bem-sucedidos – mais do que os ataques de *phishing* padrão – é que os invasores realizam pesquisas extensas sobre os alvos pretendidos. Usando as informações que encontram, eles podem usar técnicas de engenharia social para criar ataques excepcionalmente personalizados que enganam o alvo, fazendo-o pensar que está recebendo e-mails e solicitações legítimas. Como consequência, mesmo alvos de alto escalão dentro das organizações, como altos executivos, podem abrir e-mails que acreditavam ser seguros. Esses tipos de erros inadvertidos permitem que os criminosos cibernéticos roubem os dados necessários para atacar a rede desejada (KASPERSKY, 2024b).

Outro ataque considerado como de alta gravidade foi o download de um arquivo compactado que continha *ransomware* o qual é um malware que, após instalado, captura os dados de um sistema e os mantêm sob uma forte camada de criptografia, o que impede o acesso aos dados. A liberação dos dados só é feita após pagamento de uma quantia estabelecida pelos cibercriminosos. Ataques de DDoS também foram realizados a fim de sobrecarregar um servidor com intuito de tirá-lo do ar (ROHR; GOMES, 2016).

> Ransomware é um tipo de código malicioso que tornam inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e exige pagamento de resgate para restabelecer o acesso ao usuário e não vazar dados. Após infectar o dispositivo, exibe uma mensagem informando ao usuário o procedimento a ser seguido para restabelecer o acesso, incluindo: valor do resgate (geralmente em criptomoedas),

> prazo para pagamento, identificação do dispositivo do usuário e forma de contato com o atacante, como um link ou endereço de e-mail (Códigos MaliciososCERT.br, 2023).
>
> Uma criptomoeda é uma espécie de moeda digital que não depende de uma autoridade central para mantê-la. O nome se origina do fato de que suas transações são altamente criptografadas (normalmente em um livro-razão digital como o Blockchain), tornando as trocas bem seguras (RIBEIRO, 2022).

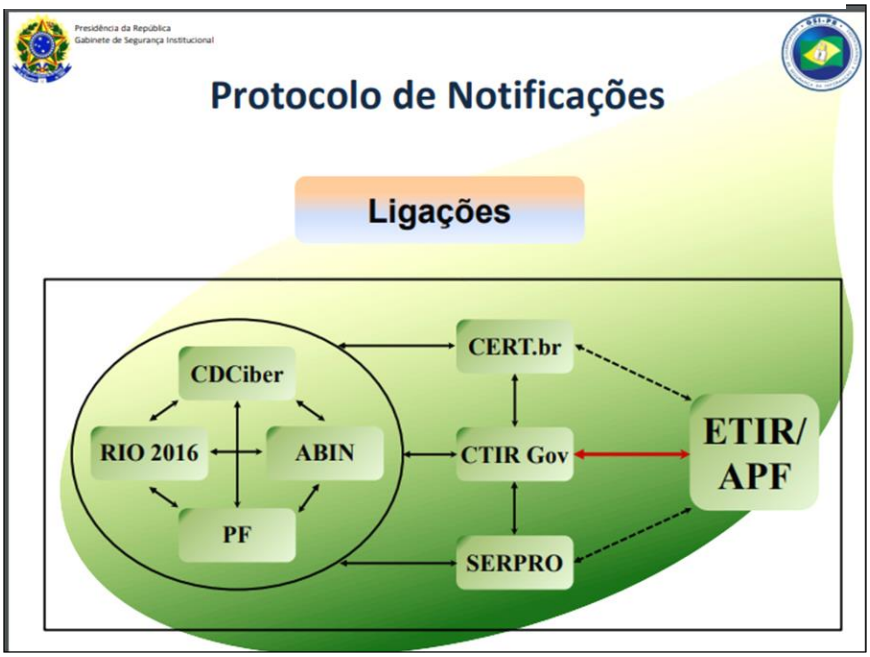
Ao todo o volume de dados trafegados na rede da Rio 2016 foi de 1,4 petabytes com quase 150.000 dispositivos conectados simultaneamente, para atender o Comitê Rio 2016, imprensa, agências de mídia, atletas, comitês olímpicos e federações. O site oficial dos jogos teve 46 milhões de visitantes, 460 milhões de visualizações de páginas e 9 bilhões de hits. Para o aplicativo móvel oficial do Rio 2016 foram mais de 5 milhões de downloads, 1 bilhão de visualizações de páginas e mais de 11 bilhões de hits (MORAES, 2016).

Vários profissionais de segurança da informação atuaram para garantir a defesa cibernética dos eventos da Rio 2016, para isso formou-se um CSIRT (*Computer Security Incident Response Team*) com 80 pessoas dedicadas. O Centro Operacional de Tecnologia (TOC – *Technology Operational Centre*) atuou com uma equipe multidisciplinar de quase 500 pessoas atuando 24 horas por dia e 7 dias na semana. No CSIRT do jogos foram processados mais de 12 bilhões de eventos de segurança por meio de 100 dispositivos de segurança que blindaram a infraestrutura da rede de dados do Rio 2016 (MORAES, 2016).

O Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) é considerado um "*Computer Security Incident Response Team* (CSIRT)", ou Grupo de Resposta a Incidentes de Segurança, que vem a ser uma organização responsável por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores (BRASIL, 2023d).

Durante a realização dos jogos Olímpicos e Paraolímpicos, o CTIR.gov atuou em conjunto com outros órgãos e entidades públicas para combate aos incidentes cibernéticos por meio de um protocolo de notificações conforme demonstrado na figura a seguir:

Figura 28 - Protocolo de Notificações



Fonte: (CTIR.Gov, 2016)

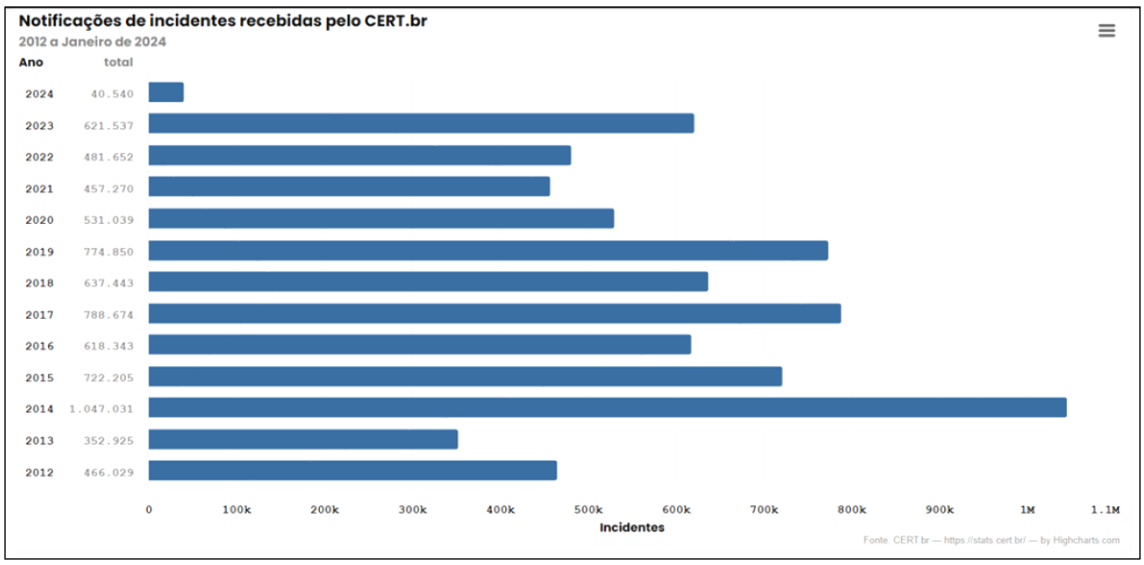
Já o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) é um CSIRT Nacional de último recurso, atua como um grupo de Resposta a Incidentes de Segurança, mantido pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br). Quanto à divisão de tarefas do Rio 2016, o CERT.br atuou para facilitar a comunicação e coordenação com outros atores e auxiliar no acompanhamento de ameaças. O CTIR.Gov focou nos ataques às redes do Governo, o CDCiber atuou presencialmente nos Centros de Comando e Controle e em redes do interesse do Ministério da Defesa e infraestruturas críticas. O CSIRT Rio 2016 trabalhou com um time 24x7 para as redes dos jogos (HOEPERS, 2017).

De acordo com dados de 2016, o CERT.br recebeu 60.432 notificações sobre computadores que participaram de ataques de negação de serviço, um aumento de 138% em relação à 2015. Já notificações de casos de páginas falsas de bancos e sítios de comércio eletrônico (*phishing*) aumentaram 37%. Por fim, as notificações de varreduras de SMTP *(Simple Mail Transfer Protocol)*, um protocolo para envio de e-mails que, quando abusado, serve para o envio de spam, eram menos de 7% do total em 2015, e em 2016 correspondeu a 30% de todas as varreduras (CERT.br, 2017).

Quando se amplia a pesquisa de computadores que participaram de ataques de DDoS para incidentes recebidos pelo CERT.BR de 2012 a janeiro de 2024, observa-se que 2014, o ano da realização da Copa do Mundo, foi o que mais recebeu notificações,

conforme demonstrado no gráfico a seguir:

Gráfico 4 - Notificações de incidentes recebidas pelo CERT.br



Fonte: (CERT.br, 2024)

Um comunicado divulgado pela Fortinet (2023), empresa especializada em segurança cibernética, notificou que a América Latina e o Caribe foram alvo de mais de 360 bilhões de tentativas de ataques cibernéticos em 2022, sendo o México o país que recebeu o maior número de tentativas de ataques (187 bilhões), seguido pelo Brasil (103 bilhões). De acordo com o comunicado, as defesas cibernéticas continuam avançando para proteger as organizações, mas os atacantes estão evoluindo suas técnicas de reconhecimento e ataques destrutivoS contra seus alvos. Em todo o ano de 2022, 73,9% dos cibercrimes foram motivados financeiramente, o que resultou no maior volume de incidentes, colocando em segundo lugar os ataques de espionagem, 13%.

Este capítulo tratou da questão do aumento de ataques cibernéticos direcionados especificamente para os grandes eventos internacionais sediados pelo Brasil, motivados principalmente por um descontentamento com o alto gasto gerado para a construção da infraestrutura necessária para atendimento das competições, como também a crescente insatisfação com a classe política.

Aproveitou-se da projeção midiática dos grandes eventos para fazer repercutir as manifestações e mobilizações sociais por meio ciberativismo. De qualquer forma, verificou-se que o impacto em termos de ataques cibernéticos não prejudicou o funcionamento do espaço cibernético brasileiro. Os eventos ocorreram sem grandes

alardes e a governança do país não foi afetada. Mesmo com o fim dos eventos como se observou nos dados estatísticos do CERT.br, o Brasil continuou sendo alvo crescente de incidentes de segurança da informação.

A história revelou que o temor do governo federal em relação aos ataques cibernéticos da Estônia, Geórgia e Stuxnet não se concretizou no país, nem mesmo as infraestruturas críticas sofreram paralisações em razão desses tipos de ataques. No entanto, serve de ponto positivo o fato de o governo brasileiro ter se mobilizado para aprimorar a sua defesa cibernética, tendo como espectro os grandes conflitos cibernéticos tratados no capítulo anterior e a execução de políticas de segurança cibernéticas abordadas no capítulo seguinte.

4. A Revolução Digital

Este capítulo inicia-se com a revisão dos conceitos referentes ao espaço cibernético e ao seu acréscimo como 5º domínio junto aos quatro já existentes: terra, ar, mar e espaço sideral. Trata também do uso do ciberespaço por mercenários. Nesse casto, entende-se por mercenários cibernéticos, *hackers*, que utilizam de programas maliciosos para a realização de atos criminosos, terroristas e danosos a sociedade.

Todos os temas supracitados são importantes para entender que o mundo virtual é um ambiente sob o qual todas as nações "navegam' para transitar informações referentes aos temas cotidianos de qualquer nação, sejam políticos, acadêmico, tecnológico, jurídico, comercial, financeiro, industrial, militar e etc. Por isso a preocupação da ONU em manter uma certa ordem no espaço cibernético, que não possui fronteiras reais e nem uma governança pré-estabelecida, não que a rede mundial de computadores tenha que ser controlada pelos governos, mas que é necessária a proposição de limites para que conflitos no ciberespaço não se transformem em uma guerra cibernética e até mesmo em uma guerra real com o uso de armamentos.

Nesse contexto, é apresentada a força cibernética brasileira sob o comando do Ministério da Defesa, que com o apoio dos Poderes Executivos e Legislativo, tem aprovado uma série de leis, decretos e portarias com a finalidade de fortalecer a sua defesa e segurança cibernéticas.

Cabe ressaltar que o orçamento do governo brasileiro para a segurança cibernética é pequeno ao compará-la ao dos Estados Unidos. O país orçou alguns milhões de reais

nos últimos anos, com uma execução orçamentária baixa. Enquanto o Departamento de Defesa americano possui um orçamento em bilhões de dólares para investir somente no domínio do ciberespaço.

4.1. O 5º domínio – Ciberespaço

Quando se pensa na questão de guerra ou conflitos cibernéticos, diferentes conceitos e definições são apresentados nas diversas frentes de estudos, sejam elas acadêmicas, jurídica, empresarial, público ou privado. A pretensão não é de se conseguir um consenso sobre o assunto, mas uma convergência quando se trata de conflito cibernético.

A percepção que se tem é que cada um atua por si só; cada nação escolhe a forma e maneira como deseja enfrentar um ataque cibernético; as regras do jogo ainda não são claras e nem bem definidas. Tem-se a impressão que as leis, acordos e regulamentações são inócuos aos fatos passados, presentes e em relação aos que ainda hão de ocorrer. O campo de pesquisa é vasto e a história ainda tateia em busca de uma conexão da guerra cinética e a cibernética.

O mundo digital impõe aos historiadores desafios que inter-relacionam o espectro técnico quanto ao conhecimento dos bits e bytes e a forma de traduzi-los para uma abrangência historicista, de fontes, fatos e dados. Uma cronologia e um sequenciamento pode ser acompanhado ao longo do desenvolvimento tecnológico, principalmente a partir da Revolução Industrial (século XIX), mas os acontecimentos que transcorrem no mundo cibernético não são descritos na forma de papel e caneta, nem se encontram em uma biblioteca ou em um arquivo privado ou público; muitas vezes são informações ainda não reveladas, fatos que ocorreram na obscuridade e imperceptíveis aos olhos humanos, muitas vezes impossíveis de serem descritos ou formatados. Alguns fatos históricos são incapazes de serem registrados até porque as fontes baseiam-se em uma matriz digital.

A história revela-nos que há pouco mais de um século, a humanidade tinha apenas dois domínios físicos nos quais operar, a terra e o mar, cada um dos quais com diferentes características físicas. O mar era utilizado por seres humanos para transporte de pessoas, comércio e para fins militares; a tecnologia desenvolvida permitia o uso de veleiros, barcos, navios a vapor. A terra, além do simples caminhar, também utilizava de tecnologias para a sua exploração como a roda, o arado, a carruagem de guerra, etc. A grande mudança ocorreu há um século, quando adicionamos um terceiro domínio físico,

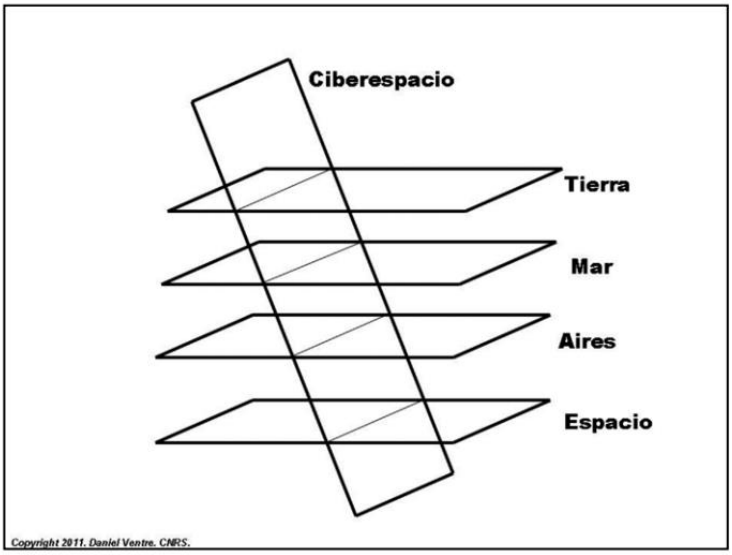
o aeroespacial. As questões bélicas no início superavam suas aplicações comerciais, os aspectos econômicos, sociais e políticos. Em 1957, o espaço sideral, mesmo que não seja tão militar ou comercialmente difundido quanto o ar, mar e terra, possui operações e atividades em todos os outros ambientes. Cada um desses quatro domínios físicos é marcado por características físicas radicalmente diferentes, e são utilizáveis apenas por meio do uso de tecnologia para explorar essas características. Recentemente adicionou-se o quinto domínio, conhecido como o ciberespaço (KUEHL, 2009).

Em consonância com as argumentações de Kuehl, para Ventre (2012, p. 34), o ciberespaço é um conceito ainda não muito bem definido, alguns acreditam ser a própria Internet, mas é algo que vai além da rede mundial de computadores e nisso incluem os satélites, os drones, os RFID, os roteadores, os aplicativos, os sistemas informatizados das indústrias, a robótica, como parte do espaço cibernético.

> A Identificação por Radiofrequência, ou RFID (Radio-Frequency Identification, na sigla em Inglês), é o método que utiliza ondas de rádio para registrar e coletar informações de etiquetas dedicadas. A tecnologia existe há décadas, mas ganhou novas aplicações e estudos mais aprofundados nos últimos anos, sendo atualmente cotada para substituir o código de barras, além de contar com algumas variações mais encorpadas já comuns no cotidiano. O RFID consiste basicamente no uso de ondas de rádio para coletar informações de objetos e até seres vivos por motivos diversos. A tecnologia foi desenvolvida originalmente durante a Segunda Guerra Mundial, pelo físico britânico Robert Alexander Watson-Watt, e utilizada pelas tropas inglesas para ampliar as capacidades dos radares (DORES, 2022).

Uma de suas características principais trata-se da transversalidade desse espaço, que perpassa por todas as dimensões convencionais (terra, ar, mar e espaço) de onde se firmam as suas raízes, por onde suas profundas ramificações se propagam, conforme demonstrado na figura 29.

Figura 29 - A interseção entre o Ciberespaço e o mundo físico

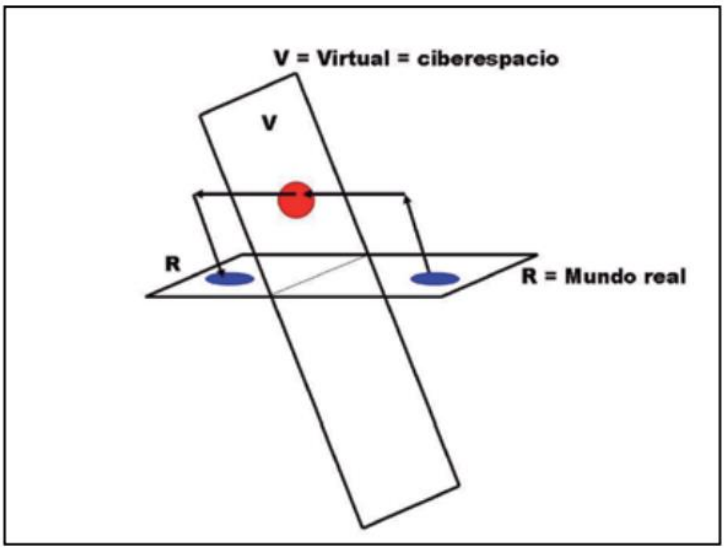


Fonte: (VENTRE, 2012, p. 34)

Em cada uma dessas quatro dimensões, a tecnologia encontra-se presente, por meio das telecomunicações, Internet, infraestrutura, computadores, softwares, aplicativos, informações, sistemas, tráfico de IP, etc.

Essas quatro áreas combinam-se dentro de um único espaço real (R) e o ciberespaço como o virtual (V). Essas dimensões cruzam-se e são nas interações desses dois mundos que ocorrem os ataques cibernéticos, figura 30 (VENTRE, 2012, p. 35).

Figura 30 - Espaço físico conectado ao ciberespaço



Fonte: (VENTRE, 2012, p. 35)

Acrescenta-se o fato de que dentro desse espaço cibernético, Ventre (2012, p. 34) menciona três camadas distintas que se comunicam:

- Uma camada inferior que trata da física, do material, do espaço da informação como da infraestrutura (hardware, redes, computadores, roteadores, switches de rede, etc).
- Uma camada intermediária que trata do software, sistemas e aplicações.
- Uma camada superior, cognitiva.

> Switches são dispositivos que tornam as conexões mais funcionais, interligando os computadores de uma maneira estruturada por meio de cabos de rede. A solução é interessante para redes domésticas mais robustas, mas principalmente no ambiente empresarial. Os equipamentos também são uma boa alternativa para quando o roteador central oferecer um número limitado de portas Ethernet (SOUSA, 2021).

Ainda segundo o Dicionário Militar do Departamento de Defesa e Termos Associados dos Estados Unidos, o ciberespaço pode ser explicado como um domínio global que inclui o ambiente da informação e suas redes interdependentes, cada uma com uma infraestrutura de tecnologia própria, que abarca a disponibilidade dos dados, o acesso à Internet, redes de telecomunicações, sistemas de computadores, processadores e controladores (Estados Unidos, 2021, p. 55). Para Kuehl (2009) esta é uma definição que retrata um contexto específico, que lida com a proteção e segurança das redes de informações militares e governamentais americanas. Outras definições de espaço cibernético encontradas em fontes de pesquisa na Internet e na literatura demonstram a diversidade de entendimento que sugere o tema, a depender do contexto onde é empregada:

Cambridge Dictionary – versão britânica	A Internet é considerada como uma área imaginária sem limites onde você pode conhecer pessoas e descobrir informações sobre qualquer assunto (CAMBRIDGE, 2022).
Cambridge Dictionary – versão norte-americana	Um sistema eletrônico que permite que usuários de computador em todo o mundo se comuniquem entre si ou acessem informações para qualquer finalidade. (CAMBRIDGE, 2022)

Pierre Lévy	O espaço cibernético é um terreno onde está funcionando a humanidade, hoje. É um novo espaço de interação humana que já tem uma importância enorme sobretudo no plano econômico e científico e, certamente, essa importância vai ampliar-se e vai estender-se a vários outros campos, como por exemplo na Pedagogia, Estética, Arte e Política. O espaço cibernético é a instauração de uma rede de todas as memórias informatizadas e de todos os computadores (LÉVY, 1994).
Techopedia	Ciberespaço refere-se ao mundo virtual do computador e, mais especificamente, um meio eletrônico que é usado para facilitar a comunicação online. O ciberespaço normalmente envolve uma grande rede de computadores composta de muitas sub-redes de computadores em todo o mundo que empregam o protocolo TCP/IP para auxiliar nas atividades de comunicação e troca de dados. A característica central do Ciberespaço é um ambiente interativo e virtual para uma ampla gama de participantes. No léxico comum de TI, qualquer sistema que tenha uma base de usuários significativa ou mesmo uma interface bem projetada pode ser considerado “ciberespaço” (ROUSE, 2023).

Departamento de Segurança da Informação do Gabinete de Segurança Institucional (DSI/GSI)	Espaço virtual composto por um conjunto de canais de comunicação da Internet e outras redes de comunicação, que garantem a interconexão de dispositivos de tecnologia da informação. Engloba todas as formas de atividades digitais em rede, incluindo o armazenamento, processamento e compartilhamento de conteúdo, além de todas as ações, humanas ou automatizadas, conduzidas por meio desse ambiente (BRASIL, 2021a)

Dentre todas as definições apresentadas, pode-se concluir que o ciberespaço vai além da Internet, não se baseia somente em uma rede aberta para tráfego de informações entre computadores, ele inclui a Internet e várias outras redes de computadores. Considerado um espaço também composto por redes transacionais que servem para enviar dados sobre fluxos de dinheiro, operações de mercado de ações, transações de cartão de crédito, etc. Também englobam sistemas de controle que acionam o funcionamento de geradores de usinas nucleares, comportas de hidrelétricas, tráfego de trens e aviações (CLARKE; KNAKE, 2015, p.88 - 89).

O espaço cibernético é um mundo paralelo, um ambiente virtual criado com a finalidade de ser independente e autogerido, sem uma necessidade específica de controle, a não ser quando envolve atos criminosos e prejudiciais às pessoas físicas e jurídicas. A quantidade de informação que trafega na rede mundial é incontável, e a cada ano cresce de forma exponencial o volume de dados trafegados nas redes corporativas, governamentais e sociais. Sem contar que a popularização e a acessibilidade da Internet disponibilizaram aos Estados-Nações muitas facilidades e avanços, mas que também impôs uma necessidade ético-relacional sobre o seu espectro de atuação.

É fato que os ataques cibernéticos ampliaram de forma considerável e de diferentes maneiras possíveis a sua forma de atuação; ninguém é inalcançável: países, instituições, sociedade, mercado financeiro, indústrias, governos, etc. Se fosse uma guerra

convencional, os danos seriam facilmente verificáveis. Como não perceber o dano causado por uma bomba? Como não contabilizar o número de mortos em combate? É simples porque é visto. Mas como contabilizar os inúmeros ataques cibernéticos aos diversos segmentos da sociedade? Seria possível dizer o número de mortos em um ataque cibernético? Roubo de informações, espionagem cibernética, adulteração de códigos e alteração de programas para fins criminosos, como visualizá-los? Sim, muitas nações estão instituindo uma nova força de defesa e ataque, uma força militar cibernética. Mas conseguiriam proteger a todos? Governo, cidadãos, indústrias, mercado financeiro, suas fontes de energia, etc.

Para Libicki (2010-, p. 05), a mensagem básica é simples:

> O ciberespaço tem seu próprio meio com suas próprias regras, sendo que os ataques cibernéticos são ativados não por meio do uso da força, mas pela exploração das vulnerabilidades do inimigo, em qualquer localização do planeta. Efeitos permanentes são difíceis de produzir. O meio está repleto de ambiguidades sobre quem atacou e por quê, sobre o que eles conseguiram e se eles podem fazê-lo novamente. Algo que funciona hoje pode não funcionar amanhã. Assim, princípios de dissuasão e combate estabelecidos em outras mídias não necessariamente traduzem de forma confiável no ciberespaço. Tais princípios devem ser repensados.

4.2. Uma nova ordem mundial

A ordem mundial cibernética do século XXI é tão complexa quanto à Guerra Fria a partir de 1947. Antes o que se tinha eram montanhas, rios e paredes separando os amigos de inimigos (SEGAL, 2016, p. 17). Atualmente, a geografia, o espaço físico importa menos que o ambiente virtual, os invasores podem agir de qualquer lugar do planeta onde exista um computador, um processador ou um cabo se conectando a uma rede.

Os guerreiros cibernéticos (CLARKE; KNAKE, 2015, p. 83) estejam na Europa, na Asia ou nas Américas, ou de qualquer outro lugar do planeta, podem usar a rede de computadores para atacar países amigos ou inimigos, sem limite de distância. Logo após o fim da Segunda Guerra Mundial, o gasto sobre o uso da força convencional era relativamente fácil de mapear, bastava delinear uma parcela da receita sobre o produto interno bruto (PIB) e sobre os gastos militares. Já o poder cibernético não é simples de se mensurar, o seu custo e gastos são uma incerteza. Ao contrário dos bombardeiros e mísseis de longo alcance, armas cibernéticas não podem ser contadas. Vale questionar se não seria melhor ter um grande corpo de tropas cibernéticas ou, dada a importância da criatividade e habilidade, um menor número de *hackers* de elite (SEGAL, 2016, p. 17).

O que torna o problema mais complexo é que não se consegue saber realmente quem é que está atacando ou o que o agressor está planejando. Sem atribuição de responsabilidade, sem saber quem está por trás de um ataque, é difícil, se não impossível, determinar quem punir, o que, por sua vez, torna mais complicado impedir um ataque cibernético (SEGAL, 2016, p. 19).

> Esta dificuldade de atribuição poderia significar que países, ao tentar identificar seus atacantes, talvez precisem confiar mais em técnicas tradicionais de inteligência, tais como invasão espiã de organizações do oponente ou métodos policiais. Ao contrário do mundo cibernético, a inteligência humana não se move à velocidade da luz. Respostas rápidas podem não estar disponíveis. Na estratégia de guerra nuclear, a atribuição não foi pensada como um grande problema, pois era possível dizer a origem de um míssil ou bombardeiro. Um ataque cibernético pode ser semelhante a uma mala-bomba indo em direção a uma cidade americana. Se avistássemos o ataque cibernético sendo lançado, de forma equivalente a silos de mísseis e bombas, poderíamos ser capazes de atribuir o ataque com um alto grau de certeza. Mas se o ataque se origina em servidores dos Estados Unidos, pode-se levar um tempo até dizer ao presidente quem nos atacou. Quanta certeza você precisa ter antes de revidar? A resposta provavelmente dependerá de circunstâncias do mundo real no momento (CLARKE; KNAKE, 2015, p. 234).

Para Kremer e Muller (2014, p. 89) o problema de atribuição incapacita a vítima a tomar determinadas decisões, pois não terá informações suficientes sobre os recursos cibernéticos do invasor que, por sua vez, afetarão a resposta. Esta dificuldade de identificação do inimigo ou atacante na guerra cibernética torna a guerra mais complicada. Os países só poderão garantir a defesa em uma guerra cibernética se o desenvolvimento tecnológico, por meio de softwares e programas, for capaz de rastrear de onde partiu o ataque; no entanto, tal defesa não será dirigida contra qualquer atacante em particular, será uma defesa contra qualquer intruso. Defesa em guerra cibernética não é uma tarefa fácil. A dissuasão pode ser possível se os Estados embarcarem em diferentes programas ofensivos de armas cibernéticas para contra-atacar os códigos maliciosos, mas a vítima sempre esbarrará na questão da atribuição, ou seja, contra quem se deve lançar um ataque cibernético.

Pode-se pensar que a estabilidade da Guerra Fria, por mais imperfeita, cara e frágil, repousava em parte na dissuasão nuclear entre as superpotências. Um ataque nuclear resultaria em uma resposta nuclear. Essa estabilidade no momento já não é mais a mesma que antes. Os níveis de ataques cibernéticos são crescentes e fornecem talvez a evidência mais clara de que os invasores sentem que podem operar na obscuridade e em razão disso, sem consequências ou punições. Durante o curso de uma invasão, os atacantes podem usar várias ferramentas de softwares para ocultarem sua identidade; eles podem pular de computadores diferentes (*botnets*) e rotear ataques através de redes em

diferentes países. Eles podem usar amplamente técnicas conhecidas e disponíveis sobre os malwares. Hackers podem conduzir "*false flag*" operações, ataques projetados para parecer que estão vindo de outro grupo ou estado-nação (SEGAL, 2016, p. 19).

> Uma operação de bandeira falsa ou "*false flag"* em inglês tem relação à guerra e conflitos violentos e refere-se à situação em que um grupo comete um ato que visa não ser responsabilizado, ou transfere a culpa para outra parte para justificar um ataque de invasão (KNORR-EVANS, 2022).

Em abril de 2015, o canal de televisão francês TV5 Monde foi retirado do ar, por atacantes alegando ser do Cyber Califado ligado ao chamado Estado Islâmico (IS[31]). Na época, associou ao fato que se tinha passado poucos meses do ataque ao jornal Charlie Hebdo[32] em Paris, e poderia ter sido um novo ataque do IS. Apurou-se que o ataque partiu de um software malicioso fabricado sob medida para corromper e destruir o hardware conectado à Internet que controlava as operações da estação de TV, como os sistemas de codificação usados para transmitir programas. Descobriu-se, meses depois, que os investigadores encontraram evidências que o canal de TV havia sido atacado por um grupo de *hackers* russos (CORERA, 2016).

Existem outros exemplos importantes quanto ao uso de operações de "*false flag*", um deles foi utilizado como motivo para o início da Segunda Guerra Mundial, quando soldados alemães da SS vestidos com uniformes poloneses simularam a invasão da Torre de Transmissão de Rádio de Gleiwitz, situado na fronteira entre a Alemanha e a Polônia

[31] O Estado Islâmico (IS em inglês) começou como uma organização iraquiana e esse legado molda o movimento atual. Grupos jihadistas proliferaram no Iraque após a invasão dos EUA em 2003, e muitos acabaram se unindo em torno de Abu Musab al-Zarqawi, um jihadista jordaniano que passou algum tempo no Afeganistão na década de 1990 e novamente em 2001. Embora Bin Laden tenha dado a Zarqawi capital inicial para iniciar sua organização, A princípio, Zarqawi se recusou a jurar lealdade e se juntar à Al Qaeda, pois compartilhava apenas alguns dos objetivos de Bin Laden e queria permanecer independente. Após meses de negociações, no entanto, Zarqawi prometeu sua lealdade e, em 2004, seu grupo assumiu o nome de "Al Qaeda no Iraque" para significar essa conexão. Bin Laden conseguiu uma afiliação mais importante da jihad em um momento em que o núcleo da Al Qaeda estava nas cordas, e Zarqawi conseguiu o prestígio e os contatos da Al Qaeda para reforçar sua legitimidade (BYMAN, 2015).

[32] O jornal *Charlie Hebdo* era bem mais que um meio de humor sarcástico. Ele criou e ampliou nos meios de comunicação franceses um espaço editorial que se definia como libertário, como uma casa-mata que protegia uma constelação muitíssimo diversificada dos pensamentos da esquerda não-oficial. Implicava com o catolicismo conservador, com o Partido Comunista, com a hierarquia judaica, com a extrema-direita e com o terrorismo islâmico. De certo modo, por mais que nunca tenha sido um jornal de ampla circulação, era por intermédio dele que sobrevivia nos meios de comunicação o pensamento criativo nascido nas barricadas estudantis de maio de 1968. O atentado ao jornal *Charlie Hebdo* ocorrido em 7 de janeiro de 2015 levantou um grande debate público em todo o mundo sobre o fundamentalismo e também sobre os limites da liberdade de expressão. Entretanto, antes disso, o jornal francês já tinha sido protagonista de outras polémicas relacionadas à religião islâmica, principalmente em períodos onde este jornal estampou em suas capas caricaturas do profeta Maomé (MORAES; SANTOS, 2016).

(GRAHAM, 2009). Após esse suposto ataque, tropas alemãs invadiram a Polônia no dia 1º de setembro de 1939.

O que muda na verdade é o ambiente, do mundo real para o mundo virtual, mas as estratégias ainda se mantém similares nos novos cenários da condução de um conflito de informação cibernética, que vão desde atividades criminosas (incluindo terrorismo), sabotagens, operações secretas e força militar preventiva, que se espalham mais rapidamente do que a capacidade da comunidade internacional de estabelecer regras acordadas para gerenciá-las.

> Uma das coisas mais interessantes sobre o florescente debate sobre guerra cibernética é a maneira pronta em que expõe nossa compreensão precária dos conceitos que empregamos rotineiramente em nosso discurso sobre a guerra como tal. Esforços para determinar se os ataques cibernéticos devem ser considerados atos de guerra, ou se eles são mais bem entendidos como criminalidade, espionagem, ou sabotagem, etc., são prejudicados por nosso entendimento vago do que a própria guerra significa. Mais especificamente os meios de guerra, sejam interpretadas como força ou violência, permanecem pouco exploradas e sub especificada pelos teóricos estratégicos. Assim, esses termos são normalmente usados tanto vagamente quanto de forma intercambiável, minando seu valor como ferramentas conceituais no processo. (...) Guerra cibernética é possível no sentido de que os ataques cibernéticos podem constituir atos de guerra. Este ponto só se torna evidente, no entanto, se formos claros sobre o que abrange os termos 'força' e 'violência', e sobre sua relação com a questão da letalidade. Atos de guerra envolvem a aplicação da força para produzir efeitos violentos. Esses efeitos violentos não precisam ser letais em caráter: eles podem quebrar coisas, em vez de matar pessoas, e ainda cair sob o título de guerra (STONE, 2013).

Para Segal (2016, p. 20), mesmo que o país atacado consiga rastrear de onde veio o ataque, ainda assim pairam incertezas sobre a origem final. O ataque teria sido instigado pelo governo nacional ou por um grupo de indivíduos motivados por uma razão política ou social? Foi realizado por conta própria ou teve atuação de cibercriminosos? Segal descreve uma conversa que teve com um oficial sênior de inteligência que lhe disse que "os ataques realizados por *hackers* em casa quando o trabalho termina pode se assemelhar aos que eles faziam durante o horário de trabalho". Por isso é necessária muito cautela para culpar o governo de outra nação de um ataque cibernético, pois existem muitas lacunas ainda não definidas nos conflitos cibernéticos. Líderes políticos, impulsionados pelo momento, podem acusar de maneira errônea os responsáveis pelo ataque e com isso gerar uma crise diplomática.

4.3. Os novos mercenários do século XXI

Dos tempos antigos, final do século V a.C, tem-se a narrativa apresentada na obra de literatura e história clássica grega, a Anábase de Ciro, escrita pelo historiador militar

grego Xenofonte, cuja narrativa apresenta a jornada de um grupo de 13.000 mercenários gregos que marcharam em favor de Ciro, o jovem, governante da Satrapia, Asia Menor com a finalidade de derrotar o seu irmão, Artaxerxes II, rei da Pérsia. Um exército de mercenários que ficou conhecido como miríades, expressão utilizada por Xenofonte para referir-se a um exército numeroso. Após serem derrotados, negociaram com o inimigo, os comandantes gregos foram decapitados e os mercenários escolheram um novo comandante, Xenofonte, que os conduziu em viagem de retorno a Grécia (RAMÍREZ, 2015, p. 173).

> Os gregos não conheciam o termo mercenário e o ambiente em que estavam envolvidos era muito diferente de hoje. Primeiro, a cidade-estado forjou relações sociais, econômicas e políticas particulares, nas quais os mercenários que sabemos hoje teriam pouco ou nenhum espaço, enquanto os da época ocupavam um lugar relevante na vida social, pois atuavam, por exemplo, como mediadores nas relações entre a aristocracia e os governantes do Mediterrâneo na Grécia clássica, e não apenas como combatentes. As pessoas que participavam da discussão de assuntos públicos na Assembleia (Ekklesia) eram muitas vezes os mesmos que foram para a guerra em nome de suas cidades, e isso está suficientemente documentado por Tucídides, na História das Guerras do Peloponeso e Heródoto, na História. Desta forma, a guerra era uma questão central na vida pública e uma obrigação cívica de lutar pela polis, para que a cidadania fosse honrada na guerra (Marinovic, 1988), ou seja, havia identidade entre o cidadão e o soldado porque, em última análise, eram a mesma pessoa, assim como se fala do camponês como soldado e do soldado como um camponês e o cidadão grego é definido como um soldado que possui um pedaço de terra, que vai à guerra para defender três coisas: sua cidade, sua terra e sua liberdade (vem da Grécia a relação simbiótica entre propriedade privada e a ideia de liberdade), e também trouxe suas próprias armas e recursos necessários (RAMÍREZ, 2015, p. 173).

Os mercenários sempre estiveram presentes ao longo da história, a tendência das nações sempre foram duas quando o assunto era a questão de guerra, “uma de usar os seus cidadãos para a guerra, como o fez o Império Romano e a maioria dos países após a Revolução Francesa e a outra, o uso de mercenários, como fez Aníbal e as cidades italianas do Renascimento” (PRADO, 2014, p. 22).

Para Pereyra (2007, p. 15–16) o mundo atual é aquele em que tudo se privatiza, não somente a força de trabalho para o crescimento econômico, como também a gestão privada das guerras e dos seus exércitos. As forças armadas de alguns países são constituídas por soldados voluntariados pagos por Estados. Esses exércitos organizam-se como uma empresa dedicada ao negócio militar que se especializa em contratar milhares de mercenários que se submetem aos que estão dispostos a pagar mais caro.

> Esta privatização dos exércitos e a terceirização do funcionamento dos negócios militares provocaram importantes mudanças na forma de se fazer a guerra na segunda metade do século XX e começo do século XXI. Essas transformações perpassam por uma crescente influência da gestão dos militares nos meios políticos e econômicos e

> do aumento da violência em todas as suas formas. Percebe-se o aumento constante do armamentismo o que impulsiona um grande número de conflitos bélicos ao redor do mundo. Alguns desses conflitos são de baixa intensidade com emprego de soldados mercenários e de policiais privatizados. Soldados e policiais usados para reprimir o seu próprio povo em países que vivenciam ou vivenciaram regimes ditatoriais, são requisitados para se juntarem as corporações militares privadas, não somente para funções militares, como também para interrogatórios, custódia de presos e torturadores. Sul africanos surgidos do apartheid, torturadores chilenos, salvadorenhos e colombianos (PEREYRA, 2007, p. 15–16).

Em 2014 já existiam várias empresas militares ou de segurança privadas que geravam um valor significativo por ano por meio de seus contratos. Em contrapartida ao aspecto de sigilo e discrição, atualmente muitas dessas empresas possuem portais na Internet, serviços de relações públicas e documentação para a imprensa e potenciais clientes. São empresas que oferecem serviços altamente diversificados no mercado internacional, realizando operações logística, aplicação da lei, assistência militar, aconselhamento e segurança, treinamento, educação militar, inteligência militar (PRADO, 2014, p. 23).

O que antes eram atividades e funções tradicionalmente reservadas aos membros da polícia e do exército, hoje são atividades ofertas pelas empresas privadas de segurança. Ou seja, busca-se dar um aspecto de legalidade a algo que transcende muitas vezes as leis de um país, pois são novas empresas que foram de certa forma legalmente constituídas, possuem até mesmo personalidade jurídica e dispõem de recursos humanos importantes, como comandantes efetivos e experientes que vêm da elite das instituições de maior prestigio (PRADO, 2014, p. 23).

Adiciona-se ao assunto, governos que contratam grupos específicos de *hackers*, conhecidos como mercenários cibernéticos, com a finalidade de atacar redes ou obter informações de forma ilegal. Tudo depende de quem paga mais para conseguir determinado objetivo no mundo digital.

Em 2013, a equipe da Kasperky registrou informações importantes sobre grupos de criminosos virtuais terceirizados que realizaram operações visando o roubo de informações. Foram utilizados ataques baseados em sabotagem por meio de programas maliciosos para limpar dados ou bloquear operações de infraestrutura. Comprometeram sites corporativos, realizaram ataques de DDoS com a finalidade de causar prejuízos financeiros (BRITO, 2013).

A Kaspersky publicou um relatório com estatísticas sobre ataques realizados por spam (e-mails indesejados) durante o primeiro trimestre de 2019. O Brasil é apontado

como aquele com a maior proporção de usuários que recebem mensagens de '*phishing*', que tentam convencer a vítima a informar dados pessoais (ROHR, 2019).

Maurer (2018, p. 31) menciona a figura do "*proxy"* que, em português, pode ser traduzido como o procurador/intermediário. Esse age com a finalidade de conduzir ou contribuir diretamente para uma operação cibernética ofensiva. Ou seja, um ator b (intermediário) atuando em lugar de um ator a (beneficiário) para afetar o ator c (alvo). Os atores neste caso poderiam ser um ente Estatal ou não-Estatal.

Ele descreve 04 tipos de relacionamentos, sendo que o primeiro trata-se de um Estado que atua como um ator b para beneficiar um outro Estado, que seria o ator a. Esse primeiro tipo de relacionamento é o mais amplamente visto na literatura, conhecido como mercenarismo estatal, utilizada séculos atrás. Como exemplo, a China Antiga fez uso de um estratagema de "matar com a espada emprestada". A história refere-se à um discípulo de Confúcio, no século V a.C, chamado Zi Gong, que para proteger o seu estado natal Lu do mais poderoso estado Qi, ele usou as regiões vizinhas como "facas emprestadas", fazendo que elas se voltassem uma contra a outra e também contra o estado de Qi, com o único propósito de proteger a região de Lu. Da mesma forma, a Agência Nacional de Segurança dos Estados Unidos (NSA) utilizou o quartel general de comunicações do governo britânico como um intermediário para conseguir informações dos cidadãos americanos, já que o acesso da NSA era restrito (MAURER, 2018, p. 32–33).

O segundo tipo trata do relacionamento estatal e intermediário privado, o que equivaleria ao mercado privado e a privatização de serviço, incluindo nesse caso corsários, mercenários, guerras por procuração, e ainda militares particulares e empresas de segurança. Participam também dessa categoria Estados ativistas em terrorismo e estudantes de direito internacional focados em intermediação. Um exemplo seria a Guerra Civil Espanhola que teve a participação de intermediários no conflito, em razão do grande número de participantes de outros países (MAURER, 2018, p. 33).

> Por exemplo, em uma entrevista de 2013 à Reuters, Costin Raiu, que lidera a pesquisa na Kaspersky Lab, disse: "O que temos aqui é o surgimento de pequenos grupos de mercenários cibernéticos disponíveis para realizar ataques direcionados. Na verdade, acreditamos que eles têm contratos e estão interessados em cumprir quaisquer que sejam os requisitos do contrato". A empresa havia acabado de expor uma sofisticada operação de hackers atingindo principalmente alvos na Coreia do Sul e Japão. Outros estudiosos compararam *hackers* a corsários. Os exemplos variam desde as acusações dos EUA de hackers iranianos e sírios até milícias patrocinados pelo Estado chinês (MAURER, 2018, p. 33–34).

O terceiro tipo de relacionamento é o Privado/ Intermediário Estatal, não é uma relação convencional, pois neste caso o ator beneficiário é um privado, sendo que na maioria dos casos a abordagem é centrada no Estado. Esses Estados são liderados por governos suscetíveis, cooptados pelo crime organizado, milícia, máfia, que usam o Estado como intermediador. Impera o esvaziamento das instituições estatais, que se utilizam de servidores públicos corruptos para venderem virtualmente a soberania do país. Atanas Atanasov, membro do parlamento búlgaro e ex-chefe de contra inteligência, ilustrou essa situação quando disse que "outros países têm máfia; na Bulgária a máfia tem o país" (MAURER, 2018, p. 34)

> Na Rússia, uma tendência semelhante ocorreu após o colapso do União Soviética. Klimburg apontou para a crescente influência das forças de segurança dentro o governo russo, observando que em 2006 mais de três quartos das principais figuras políticas russas tinham afiliações anteriores com a KGB ou o FSB, com "fortes ligações entre eles e elementos criminosos." Isso se alinha com uma observação feita por um entrevistado conhecedor das cenas de *hackers* ucranianos e russos: "Se vocês são uma pequena empresa, o FSB aceitará suborno e um agente do FSB supervisionará (MAURER, 2018, p. 34).

O quarto relacionamento envolve entidades privadas e intermediários privados, ou seja, sem necessariamente ter a participação de um Estado. Segundo Andrew Mumford (apud MAURER, p. 34) "a guerra por intermediação não é a única forma de conflito conduzida pelos Estados... O estabelecimento global de postos da Al-Qaeda afetou o modo pelo qual os conflitos regionais podem ser influenciados pela intermediação de células em rede" (MAURER, 2018, p. 34).

Esse tipo de contratação não é novidade no mundo cibernético; em 2008 uma empresa sul coreana concorrente da ItemBay (empresa de website de jogos) contratou os serviços da China para a realização de um ataque de negação de serviço. A ItemBay teve as suas operações paralisadas por várias semanas como parte de uma campanha de extorsão. Alguns anos mais tarde o gestor da empresa concorrente foi preso acusado de contratar esse ataque (Maurer, 2018, p.35).

Em maio de 2021, um ataque de *hackers* causou o fechamento temporário de um dos maiores oleodutos dos Estados Unidos, o que expõe uma fragilidade da infraestrutura energética norte-americana. A empresa operadora do oleoduto, Colonial Pipeline, foi vítima de um ataque de *ransomware*, um tipo de código malicioso que restringe o acesso aos sistemas da empresa, impedindo o funcionamento do transporte de combustível. O oleoduto transportava mais de 2,5 milhões de barris de óleo por dia, o que correspondia a 45% do abastecimento de diesel, gasolina e querosene de aviação da costa leste

americana (HERÉDIA, 2021). Segundo o website da BBC (2021b), esse ataque fez com que o governo americano declarasse estado de emergência.

Conforme informou Goulart (2021), a empresa decidiu pagar o resgate, cerca de 5 milhões de dólares, exigido pelo grupo conhecido como *Darkside* e que usa um *ransomware*, um software malicioso que bloqueia o sistema atacado e faz um pedido de resgate. Especialistas afirmam que a empresa pagou o resgate porque o sistema de *backup* (cópia) não funcionou ou porque o próprio *backup* estava vulnerável.

> A DarkSide atua como se fosse uma empresa, pois desenvolveu o seu próprio software que criptografa e rouba dados, e faz um treinamento de agentes que recebem um kit de ferramentas que contém o software, um *template* de ransomware que vem por e-mail, e recebem o treinamento de realização de ataques cibernéticos. Os hackers treinados então pagam à DarkSide uma porcentagem dos ganhos com seus ataques de ransomware que dão certo (BASTOS, 2021).

O website "Olhar Digital", do dia 11/09/2022, informou que o Brasil estava entre os cinco países que mais sofreram ataques *ransomware*, ocupando a quarta posição, atrás dos EUA, Japão e Taiwan. A matéria jornalística acrescentou que o setor governamental brasileiro é o mais atacado pelos cibercriminosos, seguido pelos setores de Educação e Indústria (FERREIRA, 2022).

No final de agosto de 2022, o grupo cibercriminoso Everest declarou em seu site na *deep web*[33] a informação sobre a invasão aos vários sistemas da Administração Federal, relatando que ao menos 3 terabites de informações internas foram vendidos a terceiros. Especialistas apontam em relatórios que esse grupo realiza não somente operações de extração de dados e travamento de sistemas, mas comercializam também *backdoors*[34] nos sistemas comprometidos, que podem ficar indisponíveis por meses, como também podem sofrer novos ataques (DEMARTINI, 2022).

---

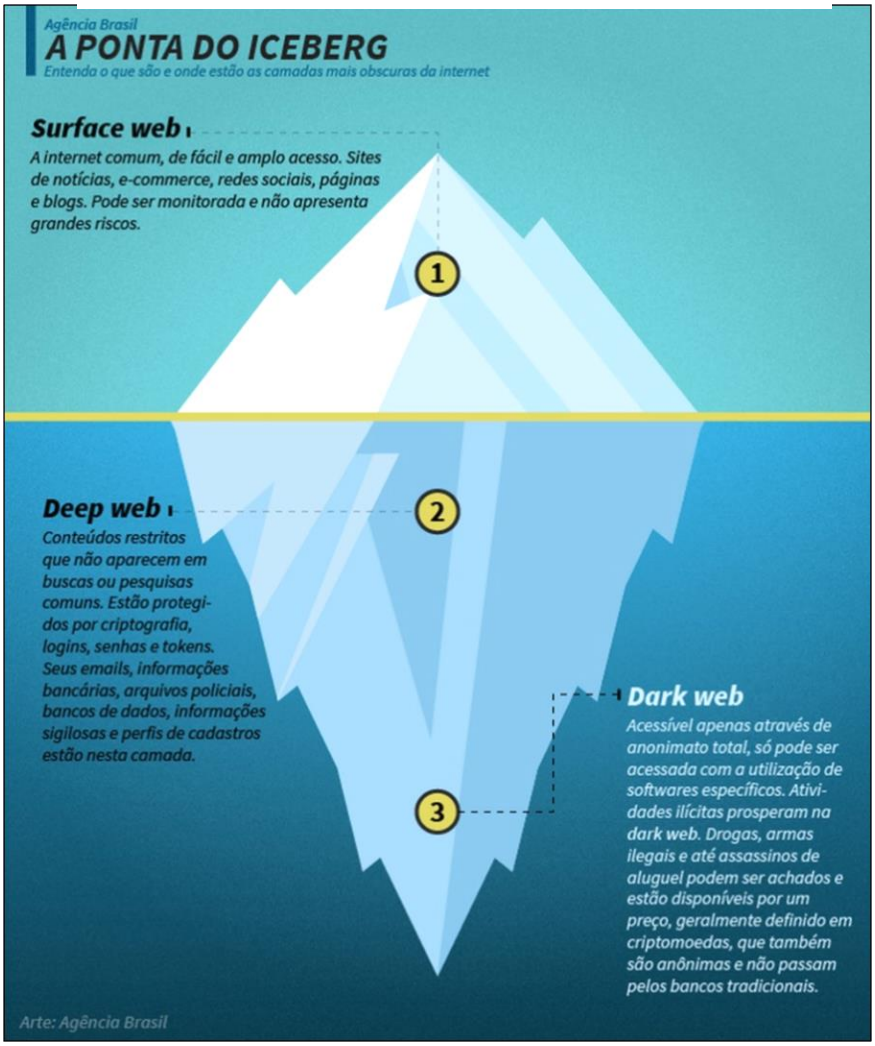
[33] Traduzida literalmente como "Internet profunda", a deep web é a camada que fica logo abaixo da Internet "rasa" - aquela que aparece nos mecanismos de busca e que fornece conteúdo aberto para qualquer pessoa conectada. Segundo a *National Public Radio* (NPR), agência pública de rádio dos Estados Unidos, mais de 90% da Internet não estão disponíveis para navegadores de "superfície", e grande parte dessa imensa fatia fica localizada na deep web. A quantidade exata de dados "escondidos" na deep web dificilmente poderia ser mensurada, já que a característica inerente dessa camada é ser restrita. Essas informações podem ser rastreadas tanto por órgãos policiais quanto por hackers. Para melhor entender, a deep web é a camada que guarda todo tipo de informação que requer senhas, logins, tokens e usa criptografia para ser acessada. As informações bancárias de um correntista, os e-mails pessoais e funcionais, os sistemas de administração de sites, blogs e redes sociais, por exemplo, podem ser considerados conteúdo *deep web* (OLIVEIRA, 2020).

[34] Permite o retorno de um invasor a um dispositivo comprometido, por meio da inclusão de serviços criados ou modificados para este fim. Pode ser incluído pela ação de outros códigos maliciosos que tenham infectado o dispositivo ou por atacantes que exploram vulnerabilidades no sistema ou aplicativos para invadi-lo (CERT.br, 2023).

Segundo Oliveira (2020), é na *dark web* (Internet obscura) que existe um mundo secreto de informações e conteúdo, que não estão disponíveis para usuários comuns, algo como um iceberg (figura 31). Em resumo, temos uma Internet de superfície que a maioria das pessoas utiliza e uma oculta, submersa. Esta, geralmente, é para atividades ilegais, tráfico para levar de drogas, material pornográfico envolvendo crianças, funcionamento de redes internacionais de pedófilos, que a utilizam para compartilhar imagens de tortura e de abusos de menores carentes. O próprio Edward Snowden, ex-agente da Central de Inteligência norte-americana (CIA) e da Agência de Segurança Nacional (NSA) transmitiu milhares de documentos secretos sobre o governo americano, que revelam grampos telefônicos e espionagem.

> O ex-analista de informática Edward Snowden que, em 2013, revelou programas secretos de espionagem em massa, disse, na primeira entrevista a uma televisão dos Estados Unidos, que recebeu treinamento de espião e trabalhou para a Central de Inteligência norte-americana (CIA) no estrangeiro. Autor da maior divulgação de documentos secretos dos últimos anos, Snowden falou de sua experiência profissional para rebater as tentativas da administração norte-americana de desvalorizar os seus conhecimentos. "Trabalhei secretamente para a CIA no estrangeiro, trabalhei secretamente para NSA [Agência de Segurança Nacional] no estrangeiro. Trabalhei para as informações militares, como professor na Academia de Contraespionagem, onde desenvolvi as fontes e os métodos para pôr em segurança as nossas informações e os nossos cidadãos nos pontos mais hostis do planeta", disse o analista, entrevistado em Moscou, onde está exilado desde agosto.(WASHINGTON, 2014)

Figura 31 - A ponta do iceberg



Fonte: (OLIVEIRA, 2020)

4.4. As tratativas da ONU sobre os ciberataques

Historicamente, na época da criação da arquitetura do ciberespaço, seus criadores não vislumbraram nem a proliferação, nem as tecnologias avançadas que iriam evoluir. Vint Cerf, um dos "pais" da Internet, se tivesse a chance de desenvolvê-la novamente, declarou o seguinte: "Eu teria colocado um foco mais forte na autenticidade ou autenticação, para saber de onde veio um determinado e-mail e de qual dispositivo foi enviado." O espaço cibernético foi construído de forma que atualmente torna-se impossível protegê-lo ou defendê-lo de ataques nocivos. Aquilo que é palpável/físico pode residir dentro de limites territoriais soberanos, o espaço virtual não. Qualquer país do mundo pode ter informações armazenadas em outros Estados, além do tráfego de informações utilizar um meio de transporte compartilhado, como satélites, antenas de

celulares, roteadores, entre outros. Isso limita a ideia de uma possível "Doutrina Monroe" no ciberespaço, a de não interferência (TRUJILLO, 2014, p. 34).

> A sexta vulnerabilidade é de a Internet ser uma grande rede com arquitetura descentralizada. Os desenvolvedores da Internet não queriam que ela fosse controlada por governos, individual ou coletivamente; assim, eles projetaram um sistema que colocou maior prioridade na descentralização e não na segurança. A ideia básica da Internet começou a se formar na década de 1960, e a Internet como é conhecida hoje é profundamente impregnada com as sensibilidades e o pensamento político da época. Enquanto muitos consideram a Internet uma invenção dos militares, ela é na verdade produto dos atualmente envelhecidos hippies dos *campi* do MIT, Stanford e Berkeley. Eles tiveram financiamento da DARPA, Agência de Projetos e Pesquisas Avançadas do Departamento de Defesa, mas a ARPANET, Rede de Projetos e Pesquisas Avançadas, não foi criada apenas para que o Departamento de Defesa se comunicasse (CLARKE; KNAKE, 2015).

Não se pode negar que a expansão cibernética é mais veloz que as tecnologias tradicionais; desenvolver armamentos cinéticos (bombas, fuzis, foguetes, aeronaves, submarinos, navios, etc) requer um alto custo e mais tempo para sua fabricação. Cabe frisar que o espaço cibernético não é limitado por fronteiras geográficas e o seu uso não é exclusivo de uma força militar. Os Estados e as sociedades para proteção dos seus interesses necessitam de que normas e regras sejam propostas e publicadas com a finalidade de implementar algum tipo de controle no mundo digital. Não se consegue impor um limite ao seu crescimento, como ocorre na expansão da indústria em relação aos níveis de desmatamento. De qualquer forma, a regulação é primordial para que injustiças e crimes sejam punidos quando cometidos. É um ambiente novo com muitas brechas jurídicas que ainda necessitam de ser preenchidas. Pois corre-se o risco, caso nada seja feito, de que os perigos e custos de atividades ilícitas sejam ampliados e impeçam o funcionamento orgânico da maioria dos Estados e sociedades (PERKOVITCH; LEVITE, 2017, p. 10).

Muitos Estados iniciaram os trabalhos para lidar com as complexidades de regular as tecnologias presentes no ciberespaço, incluindo a infraestrutura da Internet. O desafio é estabelecer regras para ações e atividades cibernéticas, que entrelaçam com a governança da Internet e a natureza da soberania no ciberespaço. Ainda que as regras sejam claras e internacionalmente aprovadas, não se pode concluir que serão suficientes para impor uma ordem no ciberespaço. Outra opção seria as iniciativas governamentais unilaterais e multilaterais para possibilitar a redução de riscos de conflitos cibernéticos irrestritos (PERKOVITCH; LEVITE, 2017, p. 10).

> Mesmo que sejam tentativas, esforços informais e formais em vários níveis, começou-se o desenvolvimento de normas para o uso de armas cibernéticas, assim como a condução

> de conflitos cibernéticos. Destacam-se aqueles oriundos de grupos como o G20 (ou Grupo dos Vinte), o Grupo de Peritos Governamentais das Nações Unidas sobre desenvolvimento no Campo da Informação e Telecomunicações no contexto da Segurança Internacional e os participantes do Manual de Tallinn[35] sobre o Direito Internacional Aplicável à Guerra Cibernética (PERKOVITCH; LEVITE, 2017, p. 10).

Diversas forças militares do mundo digitalizado e tecnológico, submetidos a diferentes sistemas políticos, têm reconhecido o caráter mutagênico e evolutivo do ciberespaço, globalmente aberto, livre, assim como os seus efeitos sobre as novas formas de conflitos estabelecidos. O que pode ser considerado a "cibernetização das forças armadas", ou seja, a formação de comandos cibernéticos nacionais ou seus equivalentes. Os formuladores de diversos países já elaboraram ou estão escrevendo políticas nacionais de segurança cibernética, normativos e leis.

> Os governos nacionais têm a responsabilidade de fornecer, regular e manter a segurança nacional, o que inclui segurança cibernética ou segurança humana para seus cidadãos (Jablonsky, 2001). David Jablonsky (2001) define segurança nacional como parte da política do governo com o objetivo de criar condições políticas favoráveis à proteção ou à extensão de valores nacionais vitais contra os existentes ou potenciais adversários. Ele estende esta definição adicionando os respectivos elementos da base de poder do estado e as prioridades que são vistas como de interesse vital e/ou nacional.
>
> (...) O ciberpoder também é definido como o emprego estratégico de tecnologias de informação e comunicação para permitir o crescimento econômico, capacitar a sociedade e aumentar a segurança (McConnell, 2012). Enquanto o ciberespaço é o domínio no qual ocorrem as operações cibernéticas, o ciberpoder é a soma de efeitos gerados por operações cibernéticas no e a partir do ciberespaço. Uma definição frequentemente usada é "ciberpoder é a capacidade de usar o ciberespaço para criar vantagens e influenciar eventos em outros ambientes operacionais e através dos instrumentos de poder" (Kuehl, 2009). Spade define o poder cibernético como "a capacidade de um estado-nação de estabelecer controle e exercer influência dentro e através do ciberespaço, em apoio e em conjunto com os outros elementos de domínio do poder nacional. Alcançar o poder cibernético depende da capacidade do Estado de desenvolver os recursos para operar no ciberespaço) (van VUUREN *et al.*, 2016).

No entanto, os pensadores das relações internacionais parecem presos às suas teorias desenvolvidas durante um sistema internacional liberal muito diferente, dominado por normas ocidentais. Tais análises de legado não capturam o mundo emergente nem

[35] Em 2019, o Centro de Excelência de Defesa Cibernética Cooperativa da Organização do Tratado do Atlântico Norte (OTAN), sigla em inglês CCDCOE – Cooperative Cyber Defence Centre of Excellence, um organismo militar internacional, localizado em Tallinn, Estônia, e creditado pela OTAN em 2008 como um 'Centro de Excelência', convidou um grupo independente de peritos internacionais para produzir um manual que trate sobre a lei que rege a guerra cibernética. Ao fazer isso, seguiu-se os passos realizados de esforços anteriores, tais como o Manual de São Remo do Instituto Internacional de Direto Humanitário que trata sobre Direto Internacional Aplicável a Conflitos Armados no Mar e Programa de Harvard sobre Política Humanitária e Manual de Pesquisa de Conflitos sobre Direito Internacional aplicável à guerra aérea e de mísseis. o projeto reuniu ilustres profissionais do direito internacional e acadêmicos em um esforço para examinar como as normas legais existentes se aplicavam a essa 'nova' forma de guerra. como seus predecessores, o manual sobre o direito internacional aplicável à guerra cibernética, ou Manual de Tallin, resulta de um processo conduzido por especialistas projetado para produzir um documento não vinculativo que aplica a lei existente à guerra cibernética (SCHMITT, 2013, p. 16).

explicam adequadamente grandes eventos, como a ascensão sem precedentes da China em uma única década (KREMER; MULLER, 2014, p. vi).

> O crescimento exponencial de Pequim no sistema econômico é um dos fatores de alteração do cenário internacional para as próximas décadas, situação em que a dinâmica das mudanças climáticas e os avanços tecnológicos definirão o contexto global do século XXI. Assim, para Xi Jinping, o desenvolvimento tecnológico torna-se imperativo, especialmente o domínio do ciberespaço em nível geral, dentro de sua visão de longo prazo de ser a economia líder no sistema internacional, definida pela política externa do Partido Comunista Chinês (PCC). Dito isso, surge a pergunta: qual seria a estratégia da China no ciberespaço, entendendo que esse é um fator determinante no futuro da ordem mundial? (CHAPARRO, 2022, p. 203).

Tendo como base a política exterior e a estratégia geopolítica, Chaparro (2022, p. 212) interpreta a pretensão da China em materializar os seus interesses e a sua influência no espaço cibernético, como forma de se contrapor ao domínio dos Estados Unidos, em duas dimensões: física e virtual.

Quanto à estratégia na dimensão virtual, o governo chinês tem realizado várias tarefas para manter a sua economia robusta, o crescimento da sua influência diplomática, bem como o seu poderio tecnológico, os quais se destacam (CHAPARRO, 2022, p. 212):

- O Partido Comunista Chinês (PCC) deseja criar uma rede muito parecida com a Internet, só que com características próprias, por meio do controle do Estado, algo como soberania cibernética. Para isso, o partido pretende por meio da empresa Huawei, uma das líderes mundiais de tecnologia, criar uma rede alternativa à Internet, conhecida como a "*New IP*", cujo objetivo seria eliminar a Internet tradicional e incluir novos modelos de governança, no qual os governos teriam condições de regular tudo que circula no ciberespaço. Para que isso ocorra, conta com o apoio da Rússia, Arábia Saudita e Irã.
- Para concretizar suas ideias, a China tem buscado o apoio da União Internacional de Telecomunicações (UIT), que faz parte da ONU, que estabelece a padronização das tecnologias de comunicação, com a finalidade de persuadi-la alegando que a Internet atual está ultrapassada e que está no limite técnico. Para isso, o PCC apresentou a "*New IP*" com sendo a nova rede de computadores para o ano de 2030, que possibilitaria a tecnologia de realidade virtual, com o uso de hologramas de tamanho natural, sistemas para carros autônomos e a cirurgia remota, pelo qual a rede atual não está apta a trabalhar com esses novos padrões.

- A China esforça-se em implementar um poderoso *"firewall"* que seja capaz de combinar a legislação e a tecnologia, com objetivo de bloquear acesso a sítios de países estrangeiros, desacelerar o tráfego da Internet transfronteiriço, limitar o acesso a fontes de informação estrangeiras e bloquear ferramentas de Internet estrangeiras.
- A China entende a complexidade e os riscos de lidar com o espaço cibernético e por isso tem atuado para restringir e penalizar as transferências comerciais como as criptomoedas (CHAPARRO, 2022, p. 212–214)

Quanto à estratégia na dimensão física, o governo chinês tem trabalhado em várias tarefas, entre as quais se destacam:

- A China empenha-se em controlar a infraestrutura de Internet, principalmente os servidores de DNS[36].
- O governo busca implementar uma Rota da Seda Digital (em inglês, DSR, cujas iniciais referem-se a Digital Silk Road). A ideia surgiu em 2015 pelo PCC e tem como proposta uma série de projetos relacionados a comercialização de equipamentos de telecomunicações e cabos de fibras óticas para países da África, Ásia, Europa, América Latina, Caribe e Reino Unido.
- Por meio da DSR, a China busca expandir-se no cenário mundial; são diversos novos atores tecnológicos com fins mais econômicos do que geopolíticos, tais como: serviços na nuvem e empresas de pagamentos, redes sociais, desenvolvedores de dispositivos inteligentes e fabricantes de drones.
- A Huawei possui 91 contratos para fornecer equipamentos de telecomunicações sem fio de tecnologia 5G[37] em todo o mundo, o que inclui 47 países da Europa, apesar das divergências com os Estados

[36] Os servidores DNS (Domain Name System, ou Sistema de Nomes de Domínios) são os responsáveis por localizar e traduzir para números IP (Internet Protocol) os endereços dos sites que digitamos nos navegadores — como www.canaltech.com.br, por exemplo. Os servidores DNS são capazes de converter as solicitações da URL em endereços de IP. Mais especificamente, eles controlam quais servidores os usuários podem acessar ao digitar um nome de domínio no browser (COSTA, 2022).

[37] O 5G é a quinta geração das redes móveis, que vem sendo desenvolvida desde os anos 2000, para ser a sucessora da rede 4G. Ela promete maiores velocidades de conexão e download de dados, entre 600 Mb/s a até 2 Gb/s. Após vários anos de desenvolvimento e especulações, entrou em operação em 2019, ainda que de forma bastante limitada (GOGONI, 2019).

Unidos, que advertia que a participação da Huawei equivaleria a dar acesso a segredos de segurança nacional aos chineses, o que foi contestado pela companhia asiática.

- A tecnologia 5G constituiria uma base tecnológica capaz de realizar uma rápida mudança e inovações na cadeia de abastecimento, ampliação da espionagem com possibilidades de futuros ataques nas infraestruturas críticas, impulsionar a capacidade militar e o crescimento econômico (CHAPARRO, 2022, p. 214–215).

Além da expansão tecnológica da China, cada vez mais formuladores de políticas reconhecem a disseminação global do espaço cibernético e suas mudanças no ambiente internacional. Nações do mundo democrático e autoritário preocupados em manter segurança no ciberespaço, principalmente por ser foco de possíveis conflitos cibernéticos, tem estabelecido uma força militar para sua defesa cibernética. E com isso, comandos cibernéticos e seus equivalentes passam a atuar em uma nova dimensão. Muito embora, tanto os políticos quanto os pensadores das relações internacionais ainda falham em suas análises quanto à ascensão da China em tão pouco tempo (KREMER; MULLER, 2014, p. vi).

Para o Conselho de Segurança da Organização das Nações Unidas – ONU, o entendimento também perpassa sobre a questão do aumento expressivo das tecnologias digitais em todo o mundo, o que tem propiciado novas formas de conflitos e condições para entes estatais e não-estatais realizarem ataques que atravessam as fronteiras internacionais. Chefes de Governo, ministros, altos funcionários e membros representantes do Conselho enfatizam que o ciberespaço está sujeito ao direito internacional, conforme a Carta das Nações Unidas e o princípio da soberania do Estado. Muitos defendem a necessidade de fechar a brecha digital entre nações, enquanto outros alertaram os Estados contra ações unilaterais em relação ao uso de tecnologia da informação e comunicação – TIC (ONU, 2021).

> Kaja Kallas, primeira-ministra da Estônia, pronunciou no debate que o que se discute não é sobre tecnologia, mas como o ciberespaço pode ser usado. “Somos responsáveis por construir um futuro onde todos os atores cumpram certas obrigações em seu comportamento no ciberespaço”. Do ponto de vista da Estônia, o direito internacional existente se aplica no ciberespaço a todos os Estados responsáveis por quaisquer atos que infrinjam suas obrigações. Os resultados apresentados pelos Grupos de Peritos Governamentais e o autônomo foram consensuais e encorajadores se posicionando sobre a implementação de uma estrutura que é uma meta vital para a comunidade internacional, acompanhada de atividades regionais e capacitação. Kallas enfatizou a necessidade de

> fechar o fosso digital, chamando a atenção para o importante papel que as empresas devem desempenhar ao investir em segurança cibernética (ONU, 2021).

Segundo Basu, Poetranto e Lau (2021), os sistemas desenvolvidos pelos governos e disponibilizados aos seus cidadãos estão cada vez mais sujeitos a ataques cibernéticos, sejam quais forem os sistemas: financeiros, comunicação, saúde e segurança, etc. Acrescentam-se, a esta lista, os sistemas de infraestruturas críticas e de controle industrial, que de alguma forma estão se conectando à Internet e que ficaram suscetíveis aos atores estatais e não estatais que adquirem dispositivos (hardware e software) para desestabilizar o espaço cibernético. Na pandemia de COVID, diversos ataques foram direcionados contra organizações médicas, um exemplo claro de ataque ao sistema de saúde de uma nação.

Diversas entidades privadas e governamentais em diferentes lugares do mundo têm sido alvo de ataques cibernéticos patrocinados por entes estatais e não-estatais. Embora a população de forma geral esteja sujeita às mesmas ameaças experimentadas pelos Estados e pelas grandes corporações, a sociedade civil não possui os mesmos recursos necessários que os governos dispõem para se defenderem. A proliferação de tecnologias de informação tão importante para desenvolvimento econômico-social serve também como meio que facilita os ataques digitais, o que ameaça a segurança e a integridade da rede de computadores mundial, como também afeta a disponibilidade, integridade, confiabilidade, integridade dos dados, bem como a privacidade dos usuários da Internet, o que deveria ser no mínimo motivo de preocupação para os governos em todo o mundo.

Os Estados membros da ONU estão preocupados em elaborar normativos que imponham um comportamento responsável dos Estados no ciberespaço, a fim de manter uma certa ordem, paz e a segurança internacionais. Iniciativas foram realizadas, tal como a criação de um grupo de trabalho da ONU, conhecida como *UN Open Ended Working Group* (OEWG) que tratou sobre assuntos relacionados a tecnologia da informação e Comunicação (ICT em inglês e TIC em português), o que resultou na adoção de um relatório de consenso em março de 2021. Muito embora esse relatório de consenso não cumpra com um dos principais objetivos do grupo de trabalho: abordar as causas da instabilidade cibernética global atual. O resultado foi a elaboração de um sistema internacional ineficaz, ou seja, incapaz de responsabilizar e salvaguardar os direitos dos usuários da rede mundial de computadores e de proteger as infraestruturas críticas dos

Estados. Esse vácuo normativo de consenso pode gerar resultados imprevisíveis e danosos (BASU; POETRANTO; LAU, 2021).

Outras tentativas de se criarem regras comuns para o ciberespaço pelos Estados membros da ONU foram vislumbradas, como as propostas elaboradas em 1999 pela Rússia, cuja ideia era apresentar um conjunto de "princípios de segurança da informação internacional" ao secretário-geral da ONU, mas também não obteve êxito, por falta de apoio. Em 2004, um Grupo de Especialistas Governamentais (*Group of Governmental Experts - GGE*) foi criado com a finalidade de desenvolver normas de responsabilização quanto ao comportamento dos Estados no espaço cibernético. Desde então, seis GGEs foram formados, incluindo o GGE em 2019–2021, criado por uma resolução patrocinada pelos americanos. Dos trabalhos realizados por esse grupo, destacam-se dois pontos importantes (BASU; POETRANTO; LAU, 2021):

1. A adoção de um relatório de consenso em 2013, que tratou de um conjunto de normas fundamentais para a governança do ciberespaço ou "normas cibernéticas" e a reafirmação do direito internacional, a soberania do Estado e os direitos humanos aplicados ao ciberespaço.
2. O relatório de 2015 que tratou do princípio da não intervenção nos assuntos internos de outros Estados, como da necessidade de os países protegerem sua própria infraestrutura crítica e não realizarem ataques que danifiquem a infraestrutura crítica de outros.

No entanto, existe um impasse entre a Rússia e os Estados Unidos quanto aos objetivos sobre a criação do OEWG. Se por um lado a Rússia alia-se à China em busca de uma reanálise das normas cibernéticas existentes e ambos atuam para estabelecer novos parâmetros que se aproximem de seus interesses, os Estados Unidos e os seus aliados se opõem às ideias defendidas pela OEWG. A Rússia alega que a OEWG é mais inclusiva por envolver todos os países membros da ONU, ao contrário do GGE, que tem em seus membros uma rotatividade, de quinze a vinte e cinco membros (BASU; POETRANTO; LAU, 2021).

A questão é que se a OEWG abrange mais países membros que a GGE, também deveria ter o poder de alterar e reescrever acordos e normas cibernéticas. Muito embora os Estados Unidos concordem que OEWG possa contribuir para a elaboração de normas e leis internacionais, entendem que a sua função de tornar esse arcabouço normativo em

obrigações vinculativas é algo que extrapola o seu mandato (BASU; POETRANTO; LAU, 2021).

> Outro ponto conflitante entre os Estados membros se trata do conceito de "soberania da informação", desenvolvido principalmente pela China e Rússia. A China define, a soberania da informação (também conhecida como soberania da Internet ou soberania cibernética) como o direito de cada país de regular em seu território suas atividades de TIC conforme julgar necessário. Essa questão foi fator de crítica pelas nações democráticas liberais, que entendem esse conceito como forma de justificar o ambiente de mídia altamente restritivo e o rigoroso uso de censura, entre outras técnicas para controlar os fluxos de informação no território chinês (BASU; POETRANTO; LAU, 2021).

Basu, Poetranto e Lau em suas argumentações entendem que OEWG beneficiaria mais os interesses da Rússia e China para obtenção de um maior controle estatal sobre a Internet, com o pretexto de combater *Fake News* (notícias falsas em português). E que a GGE beneficiaria os Estados Unidos e seus aliados, com o argumento que seriam defensores de um ambiente tecnológico aberto, confiável, seguro e livre. O resultado dessa falta de acordo impossibilitou a adoção de um relatório de consenso para avanços reais no regramento para o espaço cibernético.

> Além do mundo ocidental, Estados soberanos como China, Rússia e Brasil, e organizações regionais, como a ASEAN[38], também pretendem fazer a ponte entre a prática internacional com suas próprias realidades na governança cibernética. Enquanto isso, a maioria dos países não ocidentais, por causa de sua experiência passada de ser invadido e colonizado, são bastante sensíveis a soberania e poder do Estado; portanto, eles certamente não são a favor de organizações dominadas por poderosos países ocidentais (Flonk et al. 2020, 367). No entanto, normas cibernéticas baseadas em leituras convencionais de direitos territoriais (como direitos de defender o próprio território e controlar os recursos dentro dele, bem como direitos de controlar fronteiras e regular o fluxo de pessoas e mercadorias através delas) e obrigações (como fornecer proteção mínima para todas as pessoas em seu próprio território) promovido pelo mundo não ocidental pode comprometer os fluxos globais de informação, se eles usam as normas cibernéticas como desculpa para restringir a liberdade de expressão. Dado que não existe uma correlação simples entre as fronteiras físicas e as fronteiras do estado no ciberespaço, interrupções locais na Internet devido a problemas de política ou infraestrutura podem ter impactos globais (CHEN; YANG, 2022, p. 08).

Além do que, o trabalho desenvolvido pela OEWG, que trata de sugerir regras, normas e princípios de responsabilização dos Estados, não mencionou na elaboração da proposta de resolução ações concretas quanto à prestação de contas e ao Direito Internacional Humanitário (DIH) [39], papel essencial para a preservação da segurança e estabilidade no ciberespaço, tanto em tempos de paz quanto em conflitos armados. Os

[38] Associação das Nações do Sudeste Asiático (Association of Southeast Asian Nations em inglês).

[39] O Direito Internacional Humanitário é um conjunto de normas que, procura limitar os efeitos de conflitos armados. Protege as pessoas que não participam ou que deixaram de participar nas hostilidades, e restringe os meios e métodos de combate. O Direito Internacional Humanitário (DIH) é também designado pelo «Direito da Guerra » e por « Direito dos Conflitos Armados» (CRUZ VERMELHA, 1998).

esforços para garantir um comportamento responsável do Estado terão poucos resultados sem a aplicação de mecanismos de responsabilização dos governos por ações no ciberespaço que prejudiquem a segurança e a estabilidade internacionais (BASU; POETRANTO; LAU, 2021).

O que contribui para um cenário preocupante é a falta de referências ao Direito Internacional Humanitário, que tem como cerne o regime jurídico destinado a proteger os civis em tempos de conflito armado. Cada vez mais os Estados têm trabalhado para desenvolver instrumentos capazes de realizar ataques cibernéticos ofensivos, por exemplo, por meio de algoritmos maliciosos que sejam capazes de paralisar o fornecimento de água, energia ou saúde durante conflitos armados (BASU; POETRANTO; LAU, 2021).

É preciso que sejam contabilizados os custos humanos potenciais em caso de um conflito cibernético ou até mesmo de uma guerra cibernética. Para isso, torna-se essencial incorporar essas questões sobre o DIH nas discussões sobre normas cibernéticas. A falta de referência ao DIH no relatório de consenso da OEWG pode estar atrelada a objeções de alguns países que argumentaram contra sua aplicabilidade ao ciberespaço. Cuba, apoiada pela China e pela Rússia, argumentou que a incorporação do DIH normalizaria de alguma forma a militarização do ciberespaço e legitimaria as guerras cibernéticas. Muito embora a massificação e o crescimento de recursos cibernéticos ofensivos já sejam utilizados contra uma variedade de alvos espalhados ao redor do mundo (BASU; POETRANTO; LAU, 2021).

> O presidente chinês Xi Jinping, em um discurso na Conferência Mundial da Internet de 2015 em Wuzhen, China, se postou contra a hegemonia da Internet, como também a interferência de países estrangeiros por meio da Internet em assuntos internos do Estado chinês. Por isso o interesse da China em convencer os países membros da ONU quanto à aceitação global do conceito de soberania da Internet. A postura dos Estados Unidos e de seus aliados é a de rebater esse conceito de soberania cibernética, pois entendem que abre caminhos para que Estados não democráticos desrespeitem os direitos humanos. Enquanto China e a Rússia gostariam que o OEWG criasse uma estrutura internacional vinculante sobre TICs, os Estados Unidos e os seus aliados defendem que o direito internacional vigente, complementado pelas normas voluntárias e não vinculativas, é atualmente suficiente e reflete o consenso entre os Estados. (BASU; POETRANTO; LAU, 2021).

Cabe destacar que a Assembleia Geral das Nações Unidas do dia 5 de dezembro de 2016 propôs um conjunto de regras, normas e princípios internacionais para responsabilização dos Estados membros em manter a segurança e a pacificação dos ambientes de tecnologia da informação e comunicação, bem como uma cooperação

internacional eficaz para envolvimento dos setores privados, acadêmicos e das organizações da sociedade civil. Tal proposta teve como origem os relatórios do Grupo de Peritos Governamentais em Desenvolvimento na área da Informação e Telecomunicações no Contexto da Segurança Internacional de 2013 e 2015 adotada por consenso e recomendada na resolução 71/28 intitulada "Desenvolvimentos no domínio da informação e das telecomunicações no contexto da segurança" (ONU, 2018). As propostas da Resolução são apresentadas a seguir:

I. Os Estados devem cooperar no desenvolvimento e aplicar medidas para aumentar a estabilidade e a segurança no uso das TIC e para prevenir práticas de TIC reconhecidamente prejudiciais ou que possam ameaçar à paz e à segurança internacionais. Regramento que se encontra em harmonia com os propósitos das Nações Unidas, inclusive para manter paz e segurança internacionais,

II. Os Estados devem cumprir suas obrigações internacionais em caso de atos ilícitos que lhes sejam imputáveis de acordo com o direito internacional. No entanto, a indicação de que uma atividade de TIC que foi lançada ou se origina do território ou objetos da infraestrutura de TIC de um Estado, pode ser insuficiente para atribuir a atividade desse Estado. Acusações de organização e implementação de atos ilícitos movidos contra os Estados devem ser fundamentados. Em caso de incidentes de TIC, os Estados devem considerar todas as informações relevantes, incluindo o contexto mais amplo do evento, como a definição da atribuição na área de TIC, natureza e extensão das consequências.

III. Os Estados não devem conscientemente permitir que seu território seja usado para atos internacionalmente ilícitos por meio de TICs. Os Estados não devem usar intermediários para cometer atos internacionalmente ilícitos usando TICs e devem procurar garantir que seus territórios não sejam usados por atores não estatais para cometer tais atos.

IV. Os Estados devem considerar a melhor forma de cooperar para troca informações, ajudar uns aos outros, processar o uso terrorista e criminoso da TIC e implementar outras medidas de cooperação para lidar com tais ameaças. Os Estados precisam considerar se é necessário desenvolver novas medidas a este respeito.

V. Os Estados, ao garantir o uso seguro das TICs, devem respeitar os Direitos Humanos Resoluções do Conselho 20/8 de 5 de julho de 2012 e 26/13 de 26 de junho de 2014. Na promoção, proteção e gozo dos direitos humanos na Internet, bem como Resoluções da Assembleia Geral 68/167 de 18 de dezembro de 2013 e 69/166 de 18 de dezembro de 2014 sobre o direito à privacidade na era digital, para garantir pleno respeito pelos direitos humanos, incluindo o direito à liberdade de expressão.

VI. Um Estado não deve conduzir ou apoiar conscientemente atividades de TIC contrárias às suas obrigações no contexto do direito internacional que intencionalmente danifiquem infraestrutura ou de outra forma prejudique o uso e operação de infraestrutura para atendimento ao público.

VII. Os Estados devem tomar as medidas apropriadas para proteger sua infraestrutura contra ameaças de TIC, levando em consideração a Assembleia Geral resolução 58/199 de 23 de dezembro de 2003 sobre a criação de uma cultura global de segurança cibernética e a proteção de infraestruturas críticas de informação, e outras resoluções relevantes.

VIII. Os Estados devem responder aos pedidos apropriados de assistência por outro Estado cuja infraestrutura crítica esteja sujeita a atos maliciosos de TIC. Estados devem também responder a solicitações apropriadas para mitigar atividades maliciosas de TIC destinadas a infraestrutura crítica de outro Estado emanada de seu território, com o devido respeito à soberania.

IX. Os Estados devem tomar medidas razoáveis para garantir a integridade na cadeia

de fornecimento para que os usuários finais possam ter confiança na segurança dos produtos de TIC.

X. Os Estados devem procurar prevenir a proliferação de ferramentas TIC maliciosas, assim como o uso de técnicas e funções ocultas prejudiciais.

XI. Os Estados devem encorajar a comunicação responsável de vulnerabilidades de TIC e compartilhar informações associadas sobre soluções disponíveis para tais vulnerabilidades para limitar e possivelmente eliminar ameaças potenciais às TICs e a infraestrutura.

XII. Os Estados não devem conduzir ou apoiar conscientemente atividades que prejudiquem os sistemas de informação das equipes de tratamento de resposta a emergências autorizadas (por vezes conhecido como equipes de resposta a emergências de computador ou equipes de resposta a incidente de segurança cibernética) de outro Estado. Um Estado não deve usar recursos de equipes de resposta de emergência autorizados para se envolver em atividades internacionais maliciosas.

XIII. Os Estados devem encorajar o setor privado e a sociedade civil a desempenhar um papel apropriado para melhorar a segurança e o uso das TICs, incluindo o fornecimento segurança da cadeia de produtos e serviços de TIC. Os Estados devem cooperar com o setor privado e as organizações da sociedade civil na esfera da implementação de regras de comportamento responsável no espaço de informação com em relação ao seu papel potencial.

No governo brasileiro, compete à Secretaria de Segurança da Informação e Cibernética do Gabinete de Segurança Institucional – GSI coordenar as políticas públicas de segurança da informação e cibernética, no âmbito da administração pública federal e as atividades de segurança da informação e das comunicações. Sua competência abrange planejar e supervisionar a atividade nacional de segurança da informação e cibernética, a gestão de incidentes cibernéticos e a proteção de dados. Como também avaliar os tratados e acordos internacionais com nações amigas, as políticas e diretrizes globais de organismos multilaterais e a posição brasileira nesses organismos, nos assuntos relacionados à segurança da informação e cibernética (BRASIL, 2023e).

A Secretaria de Segurança da Informação e Cibernética, organograma apresentado na figura 32, possui dois departamentos, o Departamento de Segurança da Informação e o de Segurança Cibernética, sendo que esta última é responsável em manter o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, de responsabilidade nacional, para a proteção cibernética.

Ao correlacionar os deveres da Resolução 71/28 e as competências designadas à Secretaria de Segurança da Informação e Cibernética do Gabinete de Segurança Institucional – GSI, obtém-se a seguinte tabela:

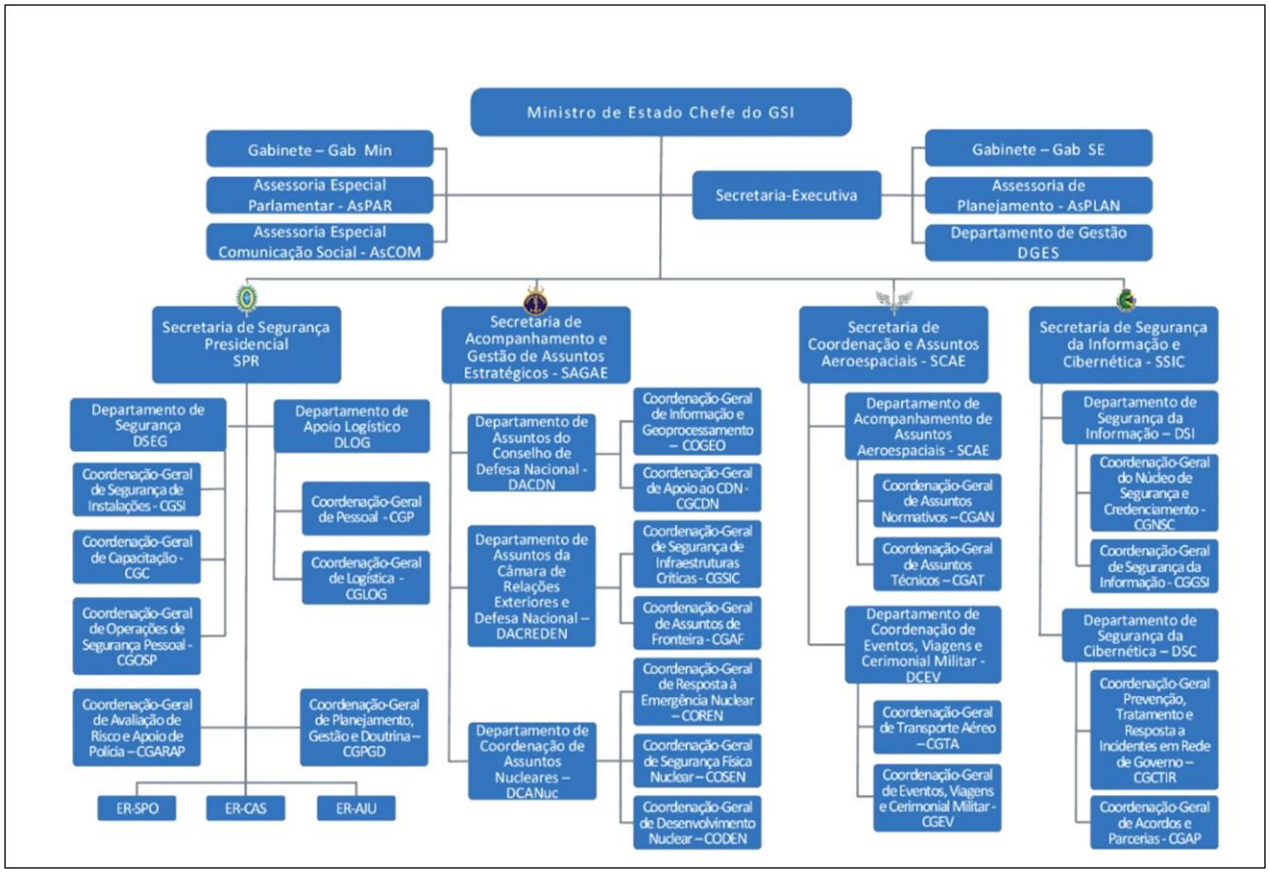
Resolução 71/28	Decreto nº 11.676/23	Análise
IV - Os Estados devem considerar a melhor forma	Inciso VI do Art. 20 e o Inciso VII do Art. 21	Em caso de um ataque de grandes proporções o

de cooperar para troca informações, ajudar uns aos outros, processar o uso terrorista e criminoso da TIC e implementar outras medidas de cooperação para lidar com tais ameaças. Os Estados precisam considerar se é necessário desenvolver novas medidas a este respeito. VIII. Os Estados devem responder aos pedidos apropriados de assistência por outro Estado cuja infraestrutura crítica esteja sujeita a atos maliciosos de TIC. Estados devem também responder a solicitações apropriadas para mitigar atividades maliciosas de TIC destinadas a infraestrutura crítica de outro Estado emanada de seu território, com o devido respeito à soberania.	(adaptado) - propor, implementar, acompanhar e avaliar tratados, acordos e outros atos internacionais relacionados à segurança da informação e à cibernética. Inciso IX do Art. 21 - assistir o Ministro de Estado no exercício das funções de Autoridade Nacional de Segurança, para o tratamento de informação classificada decorrente de tratados, acordos e outros atos internacionais, no tocante à segurança cibernética	governo brasileiro poderá solicitar apoio a outros Estados para mitigar atos maliciosos e vice-versa. O país poderá ser instado a cumprir acordos e tratados para implementar medidas de cooperação para lidar com ameaças cibernéticas.
X. Os Estados devem procurar prevenir a proliferação de ferramentas TIC maliciosas, assim	Inciso I do Art. 20 e inciso I do Art. 21 (adaptado) - planejar, coordenar e supervisionar a atividade	O governo brasileiro tem a preocupação em relação à defesa cibernética e atua para tratar os seus

como o uso de técnicas e funções ocultas prejudiciais.	nacional de segurança da informação e a segurança cibernética, a gestão de incidentes cibernéticos e a proteção de dados. Inciso III do Art. 20 e inciso III do Art. 21 (adaptado) - elaborar normativos e requisitos metodológicos relativos à atividade nacional de segurança da informação e de segurança cibernética, no âmbito da administração pública federal	incidentes de segurança da informação e cibernéticos para fins de minimizar a proliferação de ferramentas de TIC maliciosas. Atua também na elaboração de normativos de segurança da informação e cibernético que sirvam de orientação para a Administração Pública Federal.
XII. Os Estados não devem conduzir ou apoiar conscientemente atividades que prejudiquem os sistemas de informação das equipes de tratamento de resposta a emergências autorizadas (por vezes conhecido como equipes de resposta a emergências de computador ou equipes de resposta a incidente de segurança cibernética) de outro Estado. Um Estado não deve usar recursos de equipes de resposta de	Inciso IV do Art. 21 - manter o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo, de responsabilidade nacional, para a proteção cibernética; Inciso VI do Art. 21 - coordenar a Rede Federal de Gestão de Incidentes Cibernético, formada pelas equipes de prevenção, tratamento e resposta a incidentes cibernéticos dos órgãos e das entidades da administração pública	O Centro de Tratamento e Resposta a Incidentes Cibernéticos do Governo Federal tem como responsabilidade a proteção cibernética, não possui atribuição de realizar ataques cibernéticos a outro Estado e se envolver em atividades internacionais maliciosas.

emergência autorizados para se envolver em atividades internacionais maliciosas.	federal, além de outras instituições convidadas ou voluntárias	

Figura 32 - Estrutura Organizacional do GSI/PR



Fonte: (BRASIL, 2023f)

4.5. Brasil e a Defesa Cibernética

No Brasil, os assuntos relacionados às vulnerabilidades digitais foram tratados, inicialmente, sob a égide da Segurança da Informação, pelo Decreto nº 3.505/2000, que instituiu a Política de Segurança da Informação (BRASIL, 2019, p. 07). Esse Decreto foi revogado pelo Decreto nº 9.637, de 26/12/2018, que instituiu a Política Nacional de Segurança da Informação – PNSI, que abrange a defesa cibernética. O termo segurança cibernética utilizado para fins de abrangência da segurança da informação foi revogado pelo Decreto nº 11.856, de 26/12/2023 (BRASIL, 2018b), que instituiu a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança.

O governo brasileiro, em 1996, publicou a Política de Defesa Nacional – PDN,

considerada a primeira iniciativa para orientar os especialistas de toda a sociedade brasileira no sentido de reunir capacidades em nível nacional, com o objetivo de garantir a soberania do País. Em 2005 a referida política foi atualizada, e após a sua revisão em 2012, quando passou a se chamar Política Nacional de Defesa – PND, estabeleceu os Objetivos Nacionais de Defesa – OND, considerado um documento de mais alto nível para o planejamento de ações destinadas à defesa do País. Em 2008 foi publicada a primeira edição da Estratégia Nacional de Defesa – END, que orientou todos os segmentos do Estado brasileiro quanto às medidas a serem implementadas para se atingir os objetivos estabelecidos (BRASIL, 2022b, p. 07).

A Política Nacional de Defesa frisou a necessidade de uma atenção especial à segurança e à defesa do espaço cibernético brasileiro, considerados essenciais para garantir o funcionamento dos sistemas de informações, de gerenciamento e de comunicações de interesse nacional (BRASIL, 2022b, p. 14), conforme demonstrado na figura a seguir:

Figura 33 - Política Nacional de Defesa

Fonte: (BRASIL, 2013)

A Estratégia Nacional de Defesa estabeleceu três setores tecnológicos essenciais para a Defesa Nacional: o nuclear, o cibernético e o espacial. Em relação ao setor cibernético, identificaram-se, como parte prioritária, as tecnologias de comunicações entre as unidades das Forças Armadas, com a necessidade de aprimorar a Segurança da Informação e das Comunicações e a Segurança Cibernética, em todas as instâncias do Estado, principalmente no que se refere à proteção das Estruturas Críticas. Destacou-se a importância de concluir a estrutura do Sistema Militar de Defesa Cibernética com seu marco legal, suas normas e o seu emprego em todos os níveis (BRASIL, 2022b, p. 60).

O Livro Branco de Defesa (LBDN), publicado em 2020, foi inspirado no histórico dos regimes democráticos de países que adotaram esse modelo de publicação com a finalidade de expor a visão dos respectivos governos à sociedade, permitindo o acesso às informações sobre o setor, além de garantir transparência e criar novas oportunidades para o debate sobre a defesa nacional (BRASIL, 2022c) .

O LBDN destaca o cenário internacional caracterizado por incertezas que influenciam a política de defesa do Brasil. Nesse sentido, aspectos conjunturais e estruturais poderão afetar a defesa nacional como a facilidade de comunicações, principalmente a utilização de redes sociais, que permite mobilizar multidões em defesa de causas ambientais, catástrofes humanitárias, direitos humanos, entre outras. Como também podem ser utilizados para a manipulação de situações, por agentes estatais ou não estatais, no sentido de potencializar conflitos (BRASIL, 2020a, p.14-15).

> Entre os novos temas que apresentam implicações para a proteção da Soberania Nacional está a defesa cibernética. A possibilidade do surgimento de "guerras cibernéticas" no século XXI representa desafio importante para a Defesa Nacional e para a segurança internacional. A possibilidade de o País sofrer um ataque cibernético de origens das mais diversas e de difícil identificação, que poderão causar danos consideráveis a estruturas estratégicas ou mesmo a outros setores de importâncias vitais para a nação brasileira, faz com que a Defesa Cibernética passe a ter importância fundamental para a Defesa Nacional (BRASIL, 2020a, p.23).

Atualmente, o Setor Cibernético está sob coordenação do Exército brasileiro que tem alcançado avanços significativos na capacitação de pessoal especializado e no desenvolvimento de soluções de elevado nível tecnológico. Para o LBDN, a proteção do espaço cibernético abrange um grande número de áreas, como capacitação, inteligência, pesquisa científica, doutrina, preparo e emprego operacional, gestão de pessoal, além de atuar em rede (BRASIL, 2020a, p.47).

Em 2009, atendendo a determinação do Ministério da Defesa, o Exército

Brasileiro instituiu o Setor Cibernético. No ano seguinte, foi criado, pela Portaria nº 666, de 4 de agosto de 2010, o Centro de Defesa Cibernética (CDCiber); e a ativação do Núcleo do Centro de Defesa Cibernética do Exército por meio da Portaria nº 667, de 4 de agosto de 2010. Em 20 de setembro de 2012, o Decreto Presidencial nº 7.809, efetivamente incluiu o CDCiber na Estrutura Regimental do Comando do Exército (MOREIRA *et al.*, 2014, p. 92).

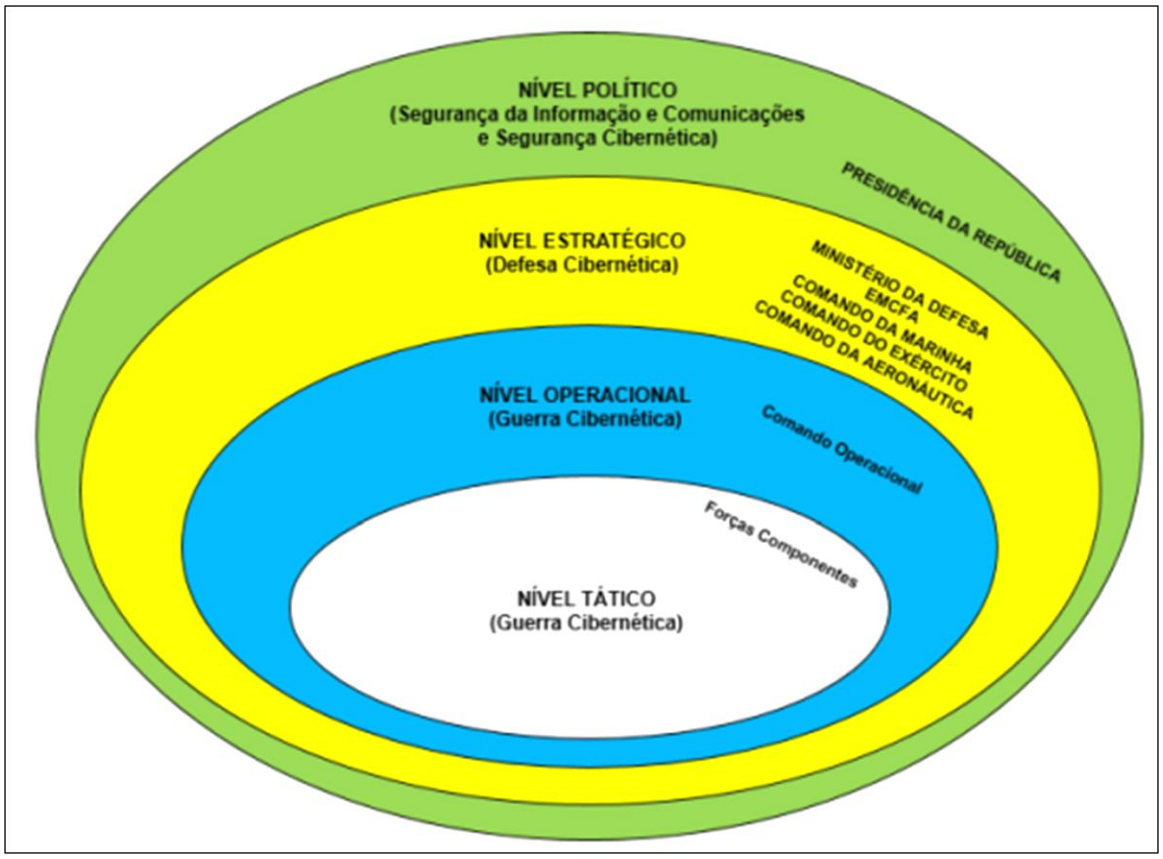
O Ministério da Defesa, por intermédio da Portaria nº 3.405/MD, de 21/12/12, atribuiu ao Centro de Defesa Cibernética, do Comando do Exército, a responsabilidade pela coordenação e pela integração das atividades de Defesa Cibernética, no âmbito do Ministério da Defesa, conforme disposto na Estratégia de Defesa Cibernética - Decreto nº 6.703, de 2008. A Portaria Normativa nº 3.389, do Ministério da Defesa, também de 21/12/12, aprovou a Política Cibernética de Defesa, entre seus objetivos estão os de desenvolver e de manter atualizada a doutrina de emprego do Setor Cibernético (BRASIL, 2014a, p. 14).

Quanto às ações no Espaço Cibernético, as seguintes denominações deverão ser seguidas, de acordo com o nível de decisão (figura 34):

- Nível político - Segurança da Informação e Comunicações e Segurança Cibernética - coordenadas pela Presidência da República e abrangendo a Administração Pública Federal direta e indireta, bem como as infraestruturas críticas da Informação Nacionais;
- Nível estratégico - Defesa Cibernética - a cargo do Ministério da Defesa, Estado Maior Conjunto das Forças Armadas e Comandos das Forças Armadas, interagindo com a Presidência da República e a Administração Pública Federal;

- Níveis operacional e tático - Guerra Cibernética - denominação restrita ao âmbito interno das Forças Armadas.

Figura 34 - Níveis de decisão



Fonte: (BRASIL, 2014a, p. 17)

Por meio da Portaria Normativa nº 2777, de 27 de outubro de 2014, o ministro da Defesa na época em exercício, Celso Amorim, estabeleceu a diretriz para implantação de medidas visando à potencialização da Defesa Cibernética Nacional (BRASIL, 2022d), com a criação do Comando de Defesa Cibernética (ComDCiber), com o exercício de militares das três forças armadas, cabendo ao Estado-Maior Conjunto das Forças Armadas (EMCFA) as atividades de coordenação nos casos de operações conjuntas; e a criação da Escola Nacional de Defesa Cibernética (ENaDCiber) na Estrutura Regimental do Comando do Exército (BRASIL, 2014b).

A missão da ENaDCiber é a de ser uma Instituição de Ensino com o foco em capacitar profissionais para exercerem funções específicas na manutenção da defesa cibernética (MOREIRA *et al.*, 2014, p. 92). A Portaria também estabelecia as ativações do Núcleo do Comando de Defesa Cibernética (NuComDCiber) e do Núcleo da Escola

Nacional de Defesa Cibernética (NuENaDCiber), ambos subordinados ao Centro de Defesa Cibernética (CDCiber).

> Em 2013, diante do emblemático caso Snowden, foi realizada uma CPI no Senado Federal sobre espionagem cibernética e foi formado um grupo de trabalho interministerial capitaneado pela Defesa, que deu origem a uma série de orientações acerca de medidas a serem tomadas para potencializar a defesa nacional no País. Assim, foram criados o Programa de Defesa Cibernética na Defesa Nacional e os núcleos da Escola Nacional de Defesa Cibernética (ENaDCiber) e do Comando de Defesa Cibernética (ComDCiber). Esse último foi ativado em 2016, quando seu primeiro comandante assumiu, sendo o expositor hoje o seu terceiro comandante. Já a Escola foi ativada em 2019 (BRASIL, 2019, p. 18).

A Doutrina Militar de Defesa Cibernética foi aprovada pela Portaria Normativa nº 3.010/MD, de 18/11/2014, além de descrever os princípios, as características, as possibilidades, as limitações, as formas de atuação de emprego da Defesa Cibernética; ela menciona também 3 tipos de ações cibernéticas:

- Ataque Cibernético - compreende ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente.
- Proteção Cibernética - abrange as ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais e redes de computadores e de comunicações, incrementando as ações de Segurança, Defesa e Guerra Cibernética em face de uma situação de crise ou conflito. É uma atividade de caráter permanente.
- Exploração Cibernética - consiste em ações de busca ou coleta, nos Sistemas de Tecnologia da Informação de interesse, a fim de obter a consciência situacional do ambiente cibernético. Essas ações devem preferencialmente evitar o rastreamento e servir para a produção de conhecimento ou identificar as vulnerabilidades desses sistemas (BRASIL, 2014a, p. 23).

A Doutrina trata de operações de Não Guerra[40], quando o emprego de ações de ataque cibernético necessita de autorização expressa de autoridade competente, normalmente em nível político máximo, no caso, a Presidência da República. Para operações de Guerra somente serão executadas as ações efetivamente necessárias conforme descrito na tabela a seguir.

Tabela 2 - Forma de atuação da defesa cibernética

FORMA DE ATUAÇÃO CIBERNÉTICA / CRITÉRIOS	POLÍTICA / ESTRATÉGICA	OPERACIONAL / TÁTICA
Nível dos Objetivos	Políticos e/ou Estratégicos	Operacionais e/ou Táticos
Foco	Obtenção de Inteligência	Preparação do campo de batalha
Nível de envolvimento nacional	Normalmente interministerial, podendo requerer ações diplomáticas e de vários ministérios e agências (Defesa, Relações Exteriores, Ciência, Tecnologia e Inovação, GSI/PR, Agência Brasileira de Inteligência - ABIN, Agência Nacional de Telecomunicações - ANATEL etc.)	Normalmente no âmbito do Ministério da Defesa, podendo contar com apoio do Ministério das Relações Exteriores
Contexto	Desde o tempo de paz, podendo fazer parte de uma Operação de Informação ou de Inteligência	Em um ambiente de crise ou conflito, apoiando uma ação militar
Nível tecnológico empregado	Normalmente alto ou muito alto	Normalmente médio ou baixo
Sincronização	Dentro do contexto de uma sofisticada Operação de Inteligência, podendo requerer ações diplomáticas anteriores ou posteriores	Dentro do contexto dos sistemas operacionais de uma Operação Militar, sincronizado com a manobra
Tempo de Preparação e Duração	Duração prolongada, com tempo de preparação normalmente mais longo, com desenvolvimento e emprego de técnicas de difícil detecção	Duração limitada, normalmente com moderado ou curto tempo de preparação, utilizando conhecimentos já levantados e técnicas previamente preparadas

Fonte: (BRASIL, 2014a, p. 23)

> As formas de atuação cibernética podem variar de acordo com o nível dos objetivos (político, estratégico, operacional ou tático), nível de envolvimento nacional, contexto de emprego, nível tecnológico empregado, sincronização e tempo de preparação. Atuação Cibernética Política/Estratégica - a atuação cibernética política/estratégica ocorre desde o tempo de paz, para atingir um objetivo político ou estratégico definido no mais alto nível, normalmente no contexto de uma Operação de Informação ou de Inteligência. Atuação Cibernética Operacional/Tática - a atuação cibernética operacional/tática é tipicamente empregada no contexto de uma Operação Militar, contribuindo para a obtenção de um efeito desejado (BRASIL, 2014a, p. 22).

Em caso de dúvidas para operações de Guerra e Não Guerra, caberá ao EMCFA consultar o nível político (Presidência da República) acerca do emprego dessas ações. Para ações de exploração cibernética, a doutrina menciona que deverão ser observados

[40] Operações em que as Forças Armadas, embora fazendo uso do Poder Militar, são empregadas em tarefas que não envolvam o combate propriamente dito, exceto em circunstâncias especiais, em que esse poder é usado de forma limitada. Podem ocorrer, inclusive, casos nos quais a expressão militar do Poder Nacional não exerça necessariamente o papel principal (BRASIL, 2014c, p. 2-9).

atos normativos do ordenamento jurídico em vigor.

O governo federal aprovou a Estratégia Nacional de Segurança Cibernética (E-Ciber), por meio do Decreto nº 10.222, de 05/02/2020, que trata de uma orientação à sociedade brasileira sobre as principais ações pretendidas, em termos nacionais e internacionais, na área da segurança cibernética durante o período de quatro anos, 2020 – 2023. É um importante instrumento de apoio ao planejamento dos órgãos e entidades do Governo para melhorar a segurança e a resiliência das infraestruturas críticas e dos serviços públicos nacionais (BRASIL, 2020b).

O E-Ciber não quer somente preencher uma lacuna apresentada no arcabouço normativo nacional sobre segurança cibernética, ele almeja também estabelecer ações com vistas a modificar, de forma cooperativa e em âmbito nacional, características que refletem o posicionamento de instituições e de indivíduos sobre o assunto. Uma de suas preocupações diz respeito à existência de boas iniciativas gerenciais nessa área, pois mostram-se fragmentadas e pontuais, o que dificulta a convergência de esforços no setor cibernético. Não há um alinhamento normativo, estratégico e operacional, o que resulta em retrabalho e consequentemente, na constituição de forças-tarefas para ações pontuais, que prejudicam a absorção de lições aprendidas e colocam em risco a eficácia prolongada dessas ações. Além do mais, a possibilidade de existência de diferentes níveis de maturidade da sociedade em segurança cibernética, resulta em percepções variadas sobre a real importância do tema (BRASIL, 2020b).

Recentemente, o governo federal assinou o Decreto nº 11.856, de 26/12/2023, que instituiu a Política Nacional de Cibersegurança (PNCiber) e o Comitê Nacional de Cibersegurança (CNCiber). Quanto aos objetivos do PNCiber, destacou-se o fomento às atividades de pesquisa científica, de desenvolvimento tecnológico e de inovação relacionadas à segurança cibernética e incrementação da atuação coordenada e o intercâmbio de informações de segurança cibernética entre a União, os Estados, o Distrito Federal e os Municípios; os Poderes Executivo, Legislativo e Judiciário; o setor privado; e a sociedade em geral. O PNCiber utiliza como instrumento a Estratégia Nacional de Cibersegurança e o Plano Nacional de Cibersegurança (BRASIL, 2023g).

De acordo com Lobo (2023), dois pontos chamaram a atenção em relação à PNCiber, o primeiro em relação a não inclusão da criação da agência nacional de cibersegurança, como pretendia o Gabinete de Segurança Institucional da Presidência da

República. O segundo, de que as estatais SERPRO e DATAPREV não foram incluídos no Comitê Nacional de Cibersegurança – CNCiber; a única agência reguladora participante foi a ANATEL.

Para Soares (2023), o governo Lula deverá propor ao Congresso projeto de lei para criar uma agência reguladora de cibersegurança. A proposta será uma das primeiras medidas tomadas pelo Comitê Nacional de Cibersegurança – CNCiber.

4.5.1 Orçamento e investimento do Brasil em Segurança Cibernética

O Tribunal de Contas da União (TCU) divulgou uma lista de alto risco da Administração Pública Federal (APF) de 2022, em fiscalização iniciada em 2020, cuja macroestrutura nacional responsável pela governança e gestão de Segurança da Informação e de Segurança Cibernética, não é adequada, pois o arcabouço normativo do GSI/PR, em especial os decretos não alcançam a Administração Pública como um todo, limitando-se, apenas, ao Poder Executivo Federal (BRASIL, 2022e).

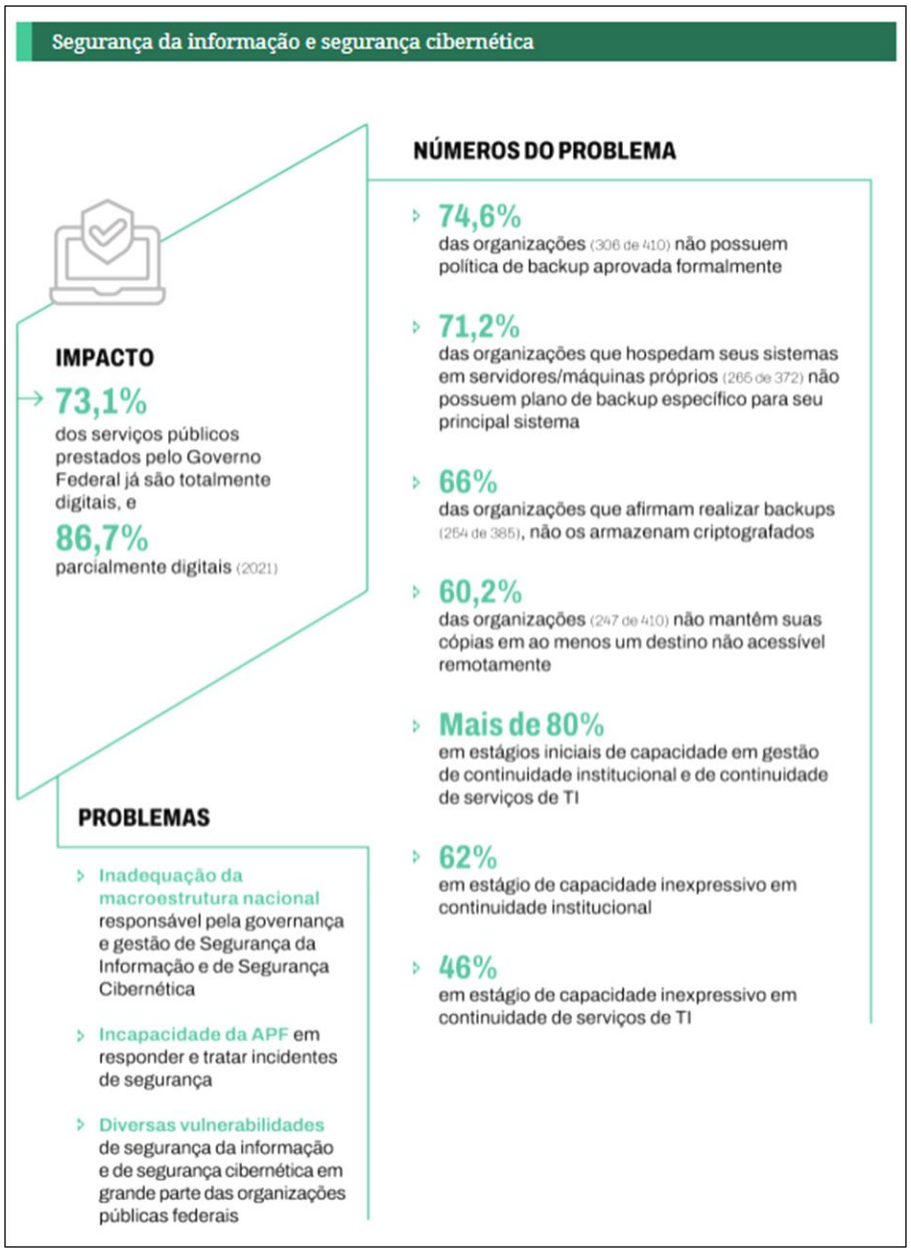
A lista menciona sobre a falta de investimentos em segurança da informação e atos normativos que regulem os temas em todo o território nacional, incluindo os setores públicos, privados e em áreas de importância estratégica para o país. O TCU entende que o cenário atual merece atenção, especialmente quanto à real capacidade da APF em responder e tratar incidentes de segurança, tanto individualmente, cada órgão e entidade, como também pela rede formada pelas equipes de tratamento de incidentes de redes (ETIRs). O investimento para o fortalecimento da defesa cibernética realizada pelo Comando de Defesa Cibernética (ComDCiber) do Exército Brasileiro está aquém da sua importância estratégica para o país.

> Em fiscalização iniciada em 2020, que avalia a suficiência e adequabilidade dos procedimentos de backup e restore de bases de dados e sistemas críticos de organizações da Administração Pública federal, o TCU constatou que:
>
> - 74,6% das organizações (306 de 410) não possuem política de backup aprovada formalmente – documento básico, negociado entre as áreas de negócio ("donas" dos dados/sistemas) e a TI da organização, com vistas a disciplinar questões e procedimentos relacionados à execução das cópias de segurança (backups);
> - 71,2% das organizações que hospedam seus sistemas em servidores/máquinas próprios (265 de 372) não possuem plano de backup específico para seu principal sistema;
> - 66% das organizações que afirmam realizar backups (254 de 385), apesar de implementarem mecanismos de controle de acesso físico ao local de armazenamento desses arquivos, não os armazenam criptografados, o que acarreta risco de vazamento de dados da organização, podendo causar enormes prejuízos, sobretudo se envolver informações sensíveis e/ou sigilosas; e

- 60,2% das organizações (247 de 410) não mantêm suas cópias em, ao menos, um destino não acessível remotamente, o que acarreta risco de que, em ataque cibernético, os próprios arquivos dos backups acabem sendo corrompidos, excluídos e/ou criptografados pelo atacante ou malware, tornando igualmente sem efeito o processo de backup/restore da organização (BRASIL, 2022e).

Em 2021, o TCU identificou que mais de 80% dos órgãos do governo brasileiro estão na fase inicial da gestão de continuidade institucional e de continuidade de serviços de TI, o cenário piora quando se verifica que a gestão de continuidade institucional é inexpressiva em 62% das instituições e a continuidade de serviços de TI é inexpressiva em 46% das instituições avaliadas no perfil de governança e gestão de TI. A figura a seguir revela os impactos relacionados aos problemas de segurança da informação nas organizações da Administração Pública Federal. Pode-se perceber que um percentual alto dessas organizações não possui políticas de segurança fundamentais para proteção dos seus ativos informacionais.

Figura 35 -Segurança da Informação e Segurança Cibernética



Fonte: (BRASIL - TCU, 2022)

Segundo o chefe do Comando de Defesa Cibernética (ComDCiber) do Exército, o General-de-Divisão Guido Amin Naves os recursos orçamentários destinados ao órgão foram muito baixos. O orçamento do ano de 2023 precisaria passar de R$ 27 milhões para R$ 150 milhões para combater a ação de *hackers*, o que ainda não seria muito se comparado aos outros programas de defesa do Estado (BRASIL, 2022f).

No relatório de gestão do Ministério da Defesa de 2021 (figura 36), o programa de defesa cibernética para a Defesa Nacional, que iniciou em 2015 e tem como data prevista para término 2035, orçou para o total do projeto o valor de R$ 3.278.700,00,

sendo que até o ano de 2021 realizou 1,6% e a realizar 98,4% do orçamento destinado ao projeto. Em relação ao ano de 2022 (figura 37) foram realizados somente 4,3% e a realizar 95,7%, cujas principais entregas até 2022 foram:

- Base Normativa para avaliação de sistemas cibernéticos de defesa e requisitos para estruturação de um observatório de defesa cibernética,
- Concepção geral do Sistema Militar de Defesa Cibernética (SMDC),
- Integração do observatório de defesa cibernética ao Observatório Militar da Praia Vermelha,
- Realização do Exercício Guardião Cibernético 3.0 (Simulação de proteção de infraestruturas críticas estratégicas),
- Serviços de certificação digital para proteção cibernética e de ampliação da capacidade cibernética da Defesa Nacional.

Uma execução orçamentária muito aquém para um projeto que tem como objetivo a manutenção do Comando de Defesa Cibernética; a capacitação de recursos humanos do Setor Cibernético; a dotação do Ministério da Defesa de estrutura necessária para desenvolver eficazmente todo o espectro das ações cibernéticas; a busca de inovações na área de Segurança da Informação e Comunicações, em especial a criptografia; a implantação de um sistema de homologação e certificação de produtos de Defesa Cibernética; e a promoção da interação com programas afins nas Forças Armadas, instituições civis públicas e privadas, e com a comunidade acadêmica nacional e internacional.

Figura 36 - Relatório de Gestão 2021 – Programa da Defesa Cibernética na Defesa Nacional

OUTRAS AÇÕES E RESULTADOS

Além dos projetos que compõem o Portfólio de Projetos Estratégicos de Defesa do MD, vale destacar:

O PROGRAMA DA DEFESA CIBERNÉTICA NA DEFESA NACIONAL, também sob responsabilidade do EMCFA, em face de sua relevância para a construção de capacidades para a Defesa Nacional, tem a finalidade de aumentar as atividades de coordenação e integração do uso do espaço cibernético, além de impedir ou dificultar sua utilização contra os interesses nacionais. Os principais objetivos são: criar e implantar o Comando de Defesa Cibernética; capacitar os recursos humanos do Setor Cibernético; dotar o MD da estrutura necessária para desenvolver eficazmente todo o espectro das ações cibernéticas; buscar inovações na área de Segurança da Informação e Comunicações, em especial a criptografia; implantar um sistema de homologação e certificação de produtos de Defesa Cibernética; e promover a interação com programas afins nas Forças Armadas, instituições civis públicas e privadas, e com a comunidade acadêmica nacional e internacional.

PROJETO ESTRATÉGICO	INÍCIO	PREVISÃO DE TÉRMINO		VALORES (R$ MILHÕES)		EXECUÇÃO FÍSICA (%)	
		INICIAL	EM DEZ/2021				
Programa da Defesa Cibernética na Defesa Nacional	2015	2035	2035	Total do projeto: Pago até 31/12/2021: PLOA 2021: Dotação 2021: LOA 2022:	3.278,7 45,0 52,1 16,6 65,9	Realizada: A realizar:	1,6 98,4

(1) PLOA 2021 - Necessidade de recursos para o exercício.

PROGRAMA DA DEFESA CIBERNÉTICA NA DEFESA NACIONAL

- Produto final: Sistema de Defesa Cibernética estruturado para atuar no espaço cibernético, de forma confiável e com liberdade de ação, para proteger-se e defender-se de ações e/ou ataques cibernéticos.
- Principais Entregas em 2021: Até 2020: Base Normativa para Avaliação de Sistemas Cibernéticos de Defesa e requisitos para estruturação de um Observatório de Defesa Cibernética. Em 2021: Concepção geral do Sistema Militar de Defesa Cibernética (SMDC); Integração do Observatório de Defesa Cibernética ao Observatório Militar da Praia Vermelha; Realização do Exercício Guardião Cibernético 3.0 (Simulação de proteção de infraestruturas críticas estratégicas); e Serviços de certificação digital para proteção cibernética e de ampliação da capacidade cibernética da Defesa Nacional.

Geração de empregos: **3.401** empregos diretos

Fonte: (BRASIL, 2021b, p. 36)

Figura 37 - Programa de Defesa Cibernética na Defesa Nacional

Programa de Defesa Cibernética na Defesa Nacional

Além dos projetos que compõem o Portfólio de Projetos Estratégicos de Defesa do MD, vale destacar o Programa de Defesa Cibernética na Defesa Nacional, sob responsabilidade do EMCFA, em face de sua relevância para a construção de capacidades para a Defesa.

Esse Projeto tem por objetivo dotar o Ministério da Defesa (MD) e as Forças Armadas (FA) da estrutura de defesa necessária para desenvolver eficazmente todo o espectro das ações cibernéticas, possibilitando atuar com liberdade de ação no espaço cibernético de interesse da Defesa Nacional e negando essa possibilidade aos oponentes.

PROJETO ESTRATÉGICO	INÍCIO	PREVISÃO DE TÉRMINO		VALORES (R$ MILHÕES)		EXECUÇÃO FÍSICA (%)	
		INICIAL	EM DEZ/2022				
Programa de Defesa Cibernética na Defesa Nacional	2015	2035	2035	Total do projeto: Pago até 31/12/2022: LOA 2022: Dotação 2022:	3.278,7 17,3 84,5 72,8	Realizada: A realizar:	4,3 95,7

Fonte: EMCFA

Geração de Empregos

3.401 Empregos diretos

5.035 Empregos indiretos

18.353 Empregos induzidos

Comando e Controle

- **Produto final:** Sistema de Defesa Cibernética estruturado para atuar no espaço cibernético, de forma confiável e com liberdade de ação, para proteção e defesa de ações e/ou ataques cibernéticos.
- **Principais entregas até 2022:** Base Normativa para avaliação de sistemas cibernéticos de defesa e requisitos para estruturação de um observatório de defesa cibernética, concepção geral do Sistema Militar de Defesa Cibernética (SMDC), integração do observatório de defesa cibernética ao Observatório Militar da Praia Vermelha, realização do Exercício Guardião Cibernético 3.0 (Simulação de proteção de infraestruturas críticas estratégicas) e serviços de certificação digital para proteção cibernética e de ampliação da capacidade cibernética da Defesa Nacional.
- **Principais entregas em 2022:** contratação da implementação integrada do Centro de Operações de Defesa Cibernética (COpDCiber-1ª fase).

Fonte: (BRASIL, 2023h, p.54)

O governo dos EUA solicitou o orçamento para despesas cibernéticas do Departamento de Defesa um total de 9,8 bilhões de dólares para 2021. No ano de 2020, o valor foi de 9,6 bilhões. Os valores orçados confirmam a importância estratégica do quinto domínio da guerra cibernética para os norte-americanos, tendo sido divididos da seguinte forma:

- Cibersegurança – US$ 5,4 bilhões
- Ciberespaço – Operações – US$ 3,8 bilhões
- Ciência e Tecnologia do Ciberespaço – US$ 556 milhões
- Além dos US$ 9,8 bilhões, o orçamento financia:
- Inteligência artificial – US$ 841 milhões
- Cloud – US$ 789 milhões

Os itens em detalhe:

- US$ 5,4 bilhões para cibersegurança – O orçamento de US$ 5,4 bilhões em segurança cibernética visa aumentar os recursos em soluções entre domínios, soluções de criptografia de última geração e modernizações de rede. O objetivo é reduzir o risco de ataques cibernéticos em redes, sistemas e informações. O valor está subdividido assim:
- US$ 678 milhões para modernização da criptografia e plataformas de próxima geração
- U$ 296,2 milhões para garantir pontos de informação e compartilhamento
- US$ 198,5 milhões para a operacionalização da modernização do Gerenciamento de Identidade e Acesso a Credenciais.
- US$ 67,2 milhões para *Comply to Connect* (C2C) e *Automated Continuous Endpoint Monitoring* (ACEM)
- US$ 69,8 milhões para infraestrutura crítica
- US$ 3,8 bilhões para operações. Esse investimento cobriria operações ofensivas e defensivas e apoiaria a implementação da Estratégia Cibernética, financiando programas e atividades. Os detalhes são:
- US$ 431,6 milhões para a cooperação com aliados e parceiros na condução de operações defensivas no ciberespaço, de "busca avançada" para combater atores cibernéticos malignos
- US$ 238,6 milhões para o desenvolvimento de capacidades para integrar comando e controle conjuntos, de coalizão e entre agências, para aprimorar as operações de vários domínios
- US$ 460,4 milhões para atividades de garantia de missão que permitam ao Departamento entender melhor os riscos de suas principais missões e aumentar a resiliência e implementar mitigações para reduzir a vulnerabilidade dos principais ativos.

O documento inclui outros US $ 2,2 bilhões para apoiar as Forças de Missões Cibernéticas (CISO, 2020).

Entre os meses de agosto de 2021 e março de 2022, o TCU realizou o primeiro de sete ciclos previstos para o acompanhamento de controles críticos de segurança cibernética das organizações públicas federais. No primeiro ciclo, foram 377 órgãos avaliados quanto à implementação de vinte medidas básicas de segurança estabelecidos pelo Centro para a Segurança da Internet (*Center for Internet Security - CIS*): inventário e controle de ativos de hardware corporativos; inventário e controle de ativos de software; gestão contínua de vulnerabilidades; conscientização sobre segurança e treinamento de competências; e gestão de respostas a incidentes.

Os questionários respondidos revelaram uma situação de alto risco para a segurança cibernética do setor público federal. As vulnerabilidades e falhas de segurança da informação e segurança cibernética ofertados pelos serviços de transformação digital aumentaram muito os riscos de ameaças e ataques cibernéticos, o que pode afetar significativamente o governo e os cidadãos (BRASIL, 2022g).

Em 2022, o TCU elaborou uma Cartilha com os "5 (cinco) controles de segurança cibernética para ontem", fruto da aplicação de uma autoavaliação de controles internos às organizações públicas federais. No primeiro ciclo de avaliação, foram avaliados cinco controles, de um total de 18 controles críticos de Segurança Cibernética (SegCiber), os quais formam um conjunto de ações de defesa de alta prioridade contra ataques cibernéticos mais pervasivos. Os gestores receberam um questionário para preencher com respostas que melhor refletissem a situação atual das respectivas organizações em relação aos cinco controles escolhidos:

■ Controle 1 – Inventário e controle de ativos corporativos: identificar e impedir a utilização de ativos de TI não autorizados/gerenciados como vetores de ataques cibernéticos.

■ Controle 2 – Inventário e controle de ativos de software: identificar e impedir a utilização de softwares não autorizados/gerenciados como vetores de ataques cibernéticos.

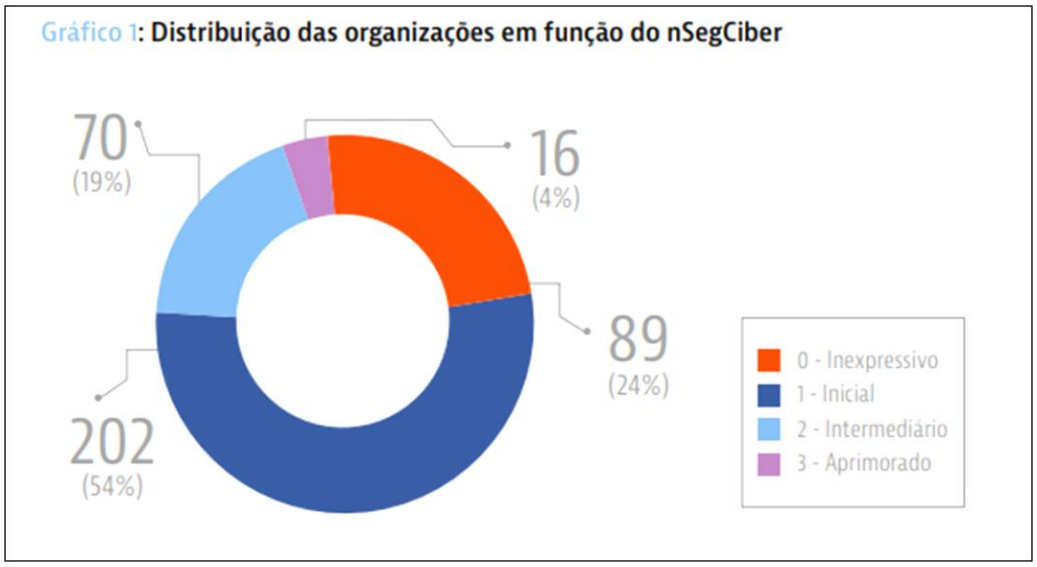
■ Controle 7 – Gestão contínua de vulnerabilidades: evitar a exploração de vulnerabilidades conhecidas nos ativos corporativos de TI.

■ Controle 14 – Conscientização sobre segurança e treinamento de competências: reduzir a possibilidade de incidentes e ataques derivados do comportamento humano – engenharia social.

■ Controle 17 – Gestão de respostas a incidentes: melhorar a capacidade de identificar potenciais ameaças e ataques, evitar que se espalhem e recuperar rapidamente dados e sistemas eventualmente corrompidos.

O panorama geral deste primeiro ciclo de avaliação foi preocupante, pois 24% das 377 organizações ainda se encontram no estágio Inexpressivo e 54%, no estágio Inicial, ou seja, pode-se afirmar que 78% das organizações ainda não implementaram devidamente os controles os 5 (cinco) controles avaliados, somente 4% encontram em estágio aprimorado. Ainda faltam avaliar 13 controles dos 18 controles críticos de Segurança Cibernética (SegCiber), conforme demonstrado na figura a seguir:

Figura 38 - Distribuição das organizações em função do nSegCiber



Fonte: (BRASIL, 2022h, p.09)

Considerações Finais

A pesquisa constatou que os conflitos cibernéticos relatados nos estudos de casos mobilizaram o governo brasileiro para fortalecer a segurança cibernética durante a realização dos grandes eventos internacionais sediados pelo país, e que esse legado tem permanecido até os dias atuais.

É importante destacar que a contextualização histórica do surgimento da informática moderna, principalmente após a Segunda Guerra Mundial, a aquisição dos primeiros computadores do Brasil, a formação de uma indústria nacional para desenvolvimento da computação, bem como, a evolução da Internet no mundo e no Brasil, serviram como base para o entendimento do funcionamento do mundo virtual.

A compreensão do conceito de espaço cibernético e as suas ramificações para todas as atividades da sociedade, sejam comerciais, financeiras, trabalhistas, governamentais, acadêmicas, etc, revelaram que qualquer abalo significativo nesse ambiente pode afetar a vida de milhões de pessoas.

Foi o que se constatou por meio dos fatos históricos apresentados, que evidenciaram, por exemplo, as vulnerabilidades do espaço cibernético da Estônia e da Geórgia. Esses países foram alvos de ataques cibernéticos intensos e constantes, durante um certo período de tempo, suficiente para desconectá-los da rede mundial de computadores, deixando-os reféns de cibercriminosos ocultos, sem que fosse possível

atribuir a responsabilidade do ataque a um ente específico.

O estudo de caso sobre a Stuxnet demonstrou que é possível atingir as estruturas críticas de uma nação mesmo que os computadores instalados não estejam conectados à Internet. Os fatos revelaram que o vírus Stuxnet foi desenvolvido especificamente para o sistema de controle de velocidade das centrífugas de enriquecimento de urânio de Natanz.

Uma única pessoa com um *pendrive* ou qualquer outro dispositivo móvel contaminado foi suficiente para disseminar o vírus para os computadores da usina nuclear e com isso alterar o código do sistema que controlava o giro de rotação das centrífugas. A partir daquele momento, o programa para enriquecimento de urânio do Irã para fins bélicos foi interrompido.

De certa forma, a inclusão dos apagões elétricos na pesquisa serviu como um alerta em relação à segurança da informação das infraestruturas críticas do Brasil. Diferentemente do que divulgou a mídia norte-americana, as evidências apresentadas, sendo uma delas por meio de um documento do Wikileaks, confirmou que a causa dos apagões se deu em razão de falhas humanas por parte do operador do sistema.

Enfim, o país temendo passar pelos mesmos problemas cibernéticos da Estônia e da Geórgia, para a realização dos grandes eventos internacionais tratou de implementar um Centro de Monitoramento Cibernético com apoio de uma força integrada entre Ministério da Justiça e Ministério da Defesa. Outra novidade no cenário brasileiro, foram a formação do Centro de Defesa Cibernética (CDCiber) e a criação da Secretaria Extraordinária de Segurança para Grandes Eventos (SESGE), que trabalharam em conjunto para a segurança cibernética e para a segurança pública.

Apesar de o país não ter sofrido um ataque cibernético na mesma proporção dos países do leste europeu, ataques de DDoS foram direcionados para vários sites governamentais e também aos patrocinadores dos eventos. Houve invasão de páginas da web e vazamento de dados, bem como ataques por meio de *spam e phishing*. Além do mais, o governo precisou lidar com uma onda de insatisfação social fomentada pelas redes sociais, em razão dos gastos despendidos para a realização e manutenção dos grandes eventos.

Concomitante aos conflitos sociais e políticos que ocorriam no país durante os eventos, o vazamento de documentos confidenciais disponibilizados por Snowden revelou que Presidência da República e assessores tinham sido alvos específicos e diretos de espionagem norte-americana. Mesmo sem constatar indícios de invasão aos sistemas do governo federal, o Congresso Nacional abriu uma CPI para investigar o caso.

Ações governamentais foram tomadas com a finalidade de nortear os rumos da cibersegurança brasileira. Foi estabelecida a Política Nacional de Defesa e a Estratégia Nacional de Defesa para propiciar uma maior estabilidade ao país e assegurar a proteção de seu território, de sua população e de setores estratégicos da economia. Para isso definiu-se como prioridade uma atenção especial para a segurança e a defesa do espaço cibernético brasileiro.

Publicou-se a Doutrina Militar de Defesa Cibernética, com a finalidade de estabelecer fundamentos necessários para tomada de decisões em caso de o país sofrer algum ataque cibernético que coloque a sua soberania sob risco. Inaugurou-se a primeira Escola Nacional de Defesa Cibernética (ENaDCIBER) na cidade de Brasília criada com a missão de fomentar e disseminar as capacitações necessárias à Defesa Cibernética e contribuir com as áreas de pesquisa e qualificar especialistas para o setor.

Recentemente, foi publicada a Política Nacional de Cibersegurança (PNCiber), com a missão de orientar a atividade de segurança cibernética no país. Ela é resultado das falhas apontadas desde 2014 pelo relatório da CPI de Espionagem Cibernética do Senado Federal. Um conjunto de necessidades foram apontadas por diferentes instituições e especialistas em cibersegurança para melhorar a governança nacional no espaço cibernético. Além de trabalhar para o desenvolvimento de uma cultura de cibersegurança nacional que abarque o setor de educação e busque a capacitação técnico-profissional em segurança cibernética.

Diante das evidências histórias investigadas, conclui-se que a aplicação da hipótese resultou na tese que a historiografia indicou que o governo brasileiro cumpriu com a missão de proteger o seu espaço cibernético durante os grandes eventos, e que esses acontecimentos contribuíram para o amadurecimento e aprimoramento da defesa cibernética brasileira.

A pesquisa também evidencia que o Brasil precisa continuar investindo em seu fortalecimento cibernético.Ppara isso é importante que realize ações conjuntas com outras nações e a ONU, tanto para troca de conhecimento tecnológico como para o estabelecimento de uma certa ordem no espaço cibernético.

Conforme demonstrado, o orçamento destinado para a defesa cibernética ainda é pouco e precisa ser repensado para que as políticas e estratégias consigam cumprir com os seus objetivos de robustecer a defesa cibernética brasileira.

Quanto aos dados apresentados pelo TCU, verificou-se que as instituições públicas necessitam de apoio para desenvolver a gestão de continuidade institucional e

de serviços e que os controles críticos de segurança cibernética precisam ser devidamente implementados.

Como sugestão para trabalhos futuros, a história tem-se mostrado essencial para a investigação dos acontecimentos ocorridos no espaço cibernético e por isso deve-se aproximar ainda mais dos eventos do mundo tecnológico, como o da inteligência artificial, a mineração de textos/dados, a aprendizagem de máquina e a cibersegurança.

Referências Bibliográficas

ABBATE, Janet. **Inventing the internet**. Cambridge - Massachusetts: MIT Press, 2000.

ADPF, Associação Nacional dos Delegados da Polícia Federal -. **Secretaria de Segurança para Grandes Eventos encerra atividades com méritos**, 2018. Disponível em: https://web.adpf.org.br/noticia/adpf/secretaria-de-seguranca-para-grandes-eventos-encerra-atividades-com-meritos/. Acesso em: 9 jan. 2024.

AGUIAR, Hugo Hotêncio de. Rússia - **1ª parte Origem e formação de um império.** Revista de informação Legislativa, 2002. Disponível em: https://www2.senado.leg.br/bdsf/handle/id/803. Acesso em: 27 fev. 2024.

ALBRIGHT, David; BRANNAN, Paul; WALROND, Christina. **Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment.** Institute for Science and International Security, 2010. Disponível em: https://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/. Acesso em: 16 fev. 2024.

ARRAES, Virgilio Caixeta; NOGUEIRA, Michel Gomes. **A Guerra Russo-Georgiana (2008): a inovação tecnológica em campo.** Meriadiano 47 - Boletim de Análise de Conjuntura em Relações Internacionais, v. 21, 2020. Disponível em: https://openurl.ebsco.com/EPDB%3Agcd%3A13%3A16999709/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Agcd%3A146019720&crl=c. Acesso em: 29 fev. 2024.

ATTA, Richard H. Van. **DARPA - The innovation icon at 60**. DARPA Defense Advanced Research Projects Agency, 2018. Disponível em: https://www.darpa.mil/attachments/DARAPA60_publication-no-ads.pdf. Acesso em: 27 fev. 2024.

_____. **Fifty years of Innovation and Discovery**. The DARPA Model for Transformative Technologies - Perspectives on the U.S. Defense Advanced Research Projects Agency, 2008. Disponível em: https://library.oapen.org/bitstream/handle/20.500.12657/23446/1/9781783747931.pdf#page=51. Acesso em: 22 nov. 2023.

BAEZNER, Marie; ROBIN, Patrice. **Stuxnet**. Zurique, Suiça: Center for Security Studies (CSS), ETH Zürich, 2017. Disponível em: https://www.research-collection.ethz.ch/handle/20.500.11850/200661. Acesso em: 16 fev. 2024.

BARKER, Daniel; FERMAINT, Kenneth; NEFF, Matthew D. **The Russo-Georgia War of 2008: Information Operations Case Study Analysis.** INTL 643 – Information Operations, 2013. Disponível em: https://www.academia.edu/11903525/The_Russia_Georgia_War_of_2008_Information_Operations_Case_Study_Analysis. Acesso em: 16 fev. 2024.

BARRETO, Pedro. **História - Rio-92.** IPEA desafios do desenvolvimento, Brasília, 2009. Disponível em: https://www.ipea.gov.br/desafios/index.php?option=com_content&id=2303:catid=28&Itemid. Acesso em: 16 fev. 2024.

BARROS, Otávio Santana Rêgo; GOMES, Ulisses de Mesquita; FREITAS, Whitney Lacerda de. **Desafios estratégicos para segurança e defesa cibernética**. 1ª ed. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011. Disponível em: https://livroaberto.ibict.br/bitstream/1/612/2/Desafios estratégicos para segurança e defesa cibernética.pdf.

BASTOS, Gustavo. Darkside, grupo hacker. **Século Diário**, 2021. Disponível em: https://www.seculodiario.com.br/colunas/darkside-grupo-hacker. Acesso em: 27 fev. 2024.

BASU, Arindrajit; POETRANTO, Irene; LAU, Justin. **The UN Struggles to Make Progress on Securing Cyberspace**, 2021. Disponível em: https://carnegieendowment.org/2021/05/19/un-struggles-to-make-progress-on-securing-cyberspace-pub-84491. Acesso em: 29 fev. 2024.

BATER, J H *et al*. **Estonia**. *In*: ENCYCLOPEDIA BRITANNICA, 2024. Disponível em: https://www.britannica.com/place/Estonia. Acesso em: 28 mai. 2024.

BBC. **Atentados de 11 de Setembro: a tragédia que mudou os rumos do século 21**, 2021a. Disponível em: https://www.bbc.com/portuguese/internacional-55351015#:~:text=Ao todo%2C 2.977 pessoas foram,aspectos%2C os rumos do mundo. Acesso em: 18 fev. 2024.

BBC, NEWS. **O ataque de hackers a maior oleoduto dos EUA que fez governo declarar estado de emergência**, 2021b. Disponível em: https://www.bbc.com/portuguese/internacional-57055618. Acesso em: 18 jan. 2024.

BERNERS-LEE, Tim. **Weaving the Web: The original design and ultimate destiny of the World Wide Web by its inventor.** 1ªed. Nova York: HarperBusiness, 1999.

BLOCH, Marc. **Apologia da história ou o ofício de historiador**. Rio de Janeiro, RJ, 2001.

BONFIM, Izac de Oliveira Belino. **Uma análise da Copa das Confederações de Futebol da FIFA 2013 sob a luz da Teoria dos Campos de Pierre Bourdieu.** PODIUM Sport, Leisure and Tourism Review, v. 2, p. 76–94, 2013. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=5037161. Acesso em: 27 fev. 2024.

BRASIL, Agência Senado. **Política Nacional de Defesa é aprovada no Senado e segue para Câmara**. Senado Notícias, 2022c. Disponível em: https://www12.senado.leg.br/noticias/materias/2022/06/02/politica-nacional-de-defesa-e-aprovada-no-senado-e-segue-para-camara. Acesso em: 24 out. 2023.

_____, Casa Civil -. **Decreto nº 11.856**, 2023g. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11856.htm#art15. Acesso em: 22 nov. 2023.

_____, CGI.br. **Decreto Nº 4.829, de 3 de setembro de 2003**, 2003. Disponível em: https://www.cgi.br/pagina/decretos/108/. Acesso em: 27 fev. 2024.

_____, CTIR.Gov. **Principais Aspectos da Segurança Cibernética relativos aos Órgãos da Administração Pública Federal nos Jogos Olímpicos e Paralímpicos RIO 2016**, 2016. Disponível em: https://www.gov.br/ctir/pt-br/centrais-de-conteudo/palestras-em-pdf/oficinas/principais-aspectos-da-seguranca-cibernetica-relativos-aos-orgaos-da-administracao-publica-federal-nos-jogos-olimpicos-e-paralimpicos-rio-2016/oficinasegurancaciberneticajogosoli. Acesso em: 20 fev. 2024.

_____, CTIR Gov. **Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo**, 2023d. Disponível em: https://www.gov.br/ctir/pt-br/acesso-a-informacao/institucional/apresentacao. Acesso em: 15 fev. 2024.

_____. **Decreto nº 70.370**, 1972. Disponível em: https://www2.camara.leg.br/legin/fed/decret/1970-1979/decreto-70370-5-abril-1972-418827-publicacaooriginal-1-pe.html. Acesso em: 19 nov. 2023.

_____. **Decreto nº 84.067**, 1979. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/1970-1979/d84067.htm. Acesso em: 18 jan. 2024.

_____. **Decreto nº 9.637/2018**, 2018b. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm#art22. Acesso em: 28 dez. 2023.

_____. **Defesa indica criação do Comando e da Escola de Defesa Cibernética**, 2022d. Disponível em: https://www.gov.br/defesa/pt-br/centrais-de-conteudo/noticias/ultimas-noticias/defesa-indica-criacao-do-comando-e-da-escola-de-defesa-cibernetica. Acesso em: 19 out. 2023.

_____. **Doutrina militar de defesa cibernética 2014**, 2014a. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31a_ma_08a_defesaa_cibernetica_1a_2014.pdf. Acesso em: 15 fev. 2024.

_____. **Emoção e honra máxima concedida ao povo do Rio e do Brasil marcam adeus dos Jogos Paralímpicos**. Rede do Esporte, 2016. Disponível em: http://rededoesporte.gov.br/pt-br/noticias/emocao-e-honra-maxima-concedida-ao-povo-do-rio-e-do-brasil-marcam-adeus-dos-jogos-paralimpicos. Acesso em: 5 dez. 2023.

_____, Gabinete de Segurança Institucional. **OSIC Orientação de Segurança da Informação Cibernética 03/2023**. **Abuso de Sítio Eletrônico de Governo - DEFACEMENT**, 2023c. Disponível em: https://www.gov.br/gsi/pt-br/ssic/osic/osic-03-23.pdf. Acesso em: 19 out. 2023.

_____, Gabinete de Segurança Institucional. **LIVRO VERDE SEGURANÇA CIBERNÉTICA NO BRASIL**, 2010. Disponível em: https://www.bibliotecadeseguranca.com.br/wp-

content/uploads/2015/10/Livro_Verde_SEG_CIBER.pdf. Acesso em: 19 out. 2023.

_____, Gabinete de Segurança Institucional. **Segurança de Infraestruturas Críticas**, 2023b. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/seguranca-de-infraestruturas-criticas#:~:text=Infraestruturas críticas são instalações%2C serviços,do Estado e da sociedade. Acesso em: 22 fev. 2024.

_____, Gabinete de Segurança Institucional. **Organograma do GSI/PR**, 2023f. Disponível em: https://www.gov.br/gsi/pt-br/composicao/organograma-1. Acesso em: 21 fev. 2024.

_____, Gabinete de Segurança Institucional. **Decreto nº 11.676**, 2023e. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11676.htm#art5. Acesso em: 15 fev. 2024.

_____ Gabinete de Segurança Institucional. **Glossário de Segurança da Informação - Espaço Cibernético**, 2021a. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/dsi/glossario-de-seguranca-da-informacao-1. Acesso em: 12 jan. 2024.

_____. **Lei 7.232/1984**, 1984. Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L7232.htm. Acesso em: 19 out. 2023.

_____. **Livro branco de Defesa Nacional**, 2020a. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/livro_branco_congresso_nacional.pdf. Acesso em: 30 jan. 2024.

_____, Ministério da Defesa. **A Política Nacional de Defesa (PND) e a Estratégia Nacional de Defesa (END)**, 2013. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/credn/arquivos/arquivos-de-apresentacoes-em-eventos/2013/abril/24-04-2013-politica-de-defesa-nacional-pdn-a-estrategia-nacional-de-defesa-end-e-o-livro-branco-de-defesa-nacio. Acesso em: 22 nov. 2023.

_____Ministério da Defesa. **Relatório de gestão integrado**, 2021b. Disponível em: https://www.gov.br/defesa/pt-br/acesso-a-informacao/transparencia-e-prestacao-de-contas/2022/rgmd21_300522.pdf. Acesso em: 19 out. 2023.

_____, Ministério da Defesa. **A Participação do Exército na Segurança dos Grandes Eventos - O Legado**, 2018a. Disponível em:

https://bdex.eb.mil.br/jspui/bitstream/1/1130/1/Grandes Eventos_O Legado.pdf. Acesso em: 5 out. 2023.

_____, Ministério da Defesa. **JMJ 2013: A participação da Defesa na Jornada Mundial da Juventude**. Gov.br, 2022a. Disponível em: https://www.gov.br/defesa/pt-br/centrais-de-conteudo/noticias/ultimas-noticias/15-07-2013-defesa-a-participacao-da-defesa-na-jornada-mundial-da-juventude. Acesso em: 23 dez. 2023.

_____, Ministério da Defesa. **Manual de Fundamentos – Operações**, 2014c. Disponível em: https://www.esao.eb.mil.br/images/Arquivos/CMB/publicacoes/manual_de_campanha_manual_de_fundamentos.pdf. Acesso em: 21 fev. 2024.

_____, Ministério da Defesa. **Relatório de Gestão 2022**, 2023h. Disponível em: https://www.gov.br/defesa/pt-br/acesso-a-informacao/transparencia-e-prestacao-de-contas/relatorio-de-gestao/arquivos-relatorio-2022/relatorio_gestao_md_2022_11052023.pdf. Acesso em: 16 jan. 2024.

_____ NIC.BR. **Exército quer novo orçamento para combater a ação de hackers**, 2022f. Disponível em: https://www.nic.br/noticia/na-midia/exercito-quer-novo-orcamento-para-combater-a-acao-de-hackers/#:~:text=A estimativa é que o,programas de defesa do Estado. Acesso em: 5 dez. 2023.

_____. **Política Nacional de Defesa e Estratégia Nacional de Defesa**, 2022b. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congressonacional_22_07_2020.pdf/view. Acesso em: 29 fev. 2024.

_____. **Portaria Normativa nº 2777**, 2014b. Disponível em: https://www.diariodasleis.com.br/legislacao/federal/228717-potencializauuo-da-defesa-cibernutica-nacional-dispue-sobre-a-diretriz-de-implantauuo-de-medidas-visando-u-potencializauuo-da-defesa-cibernutica-nacional-e-du-outras-providuncia.html. Acesso em: 30 jan. 2024.

_____. **Relatório de Avaliação de Política Pública a Política Nacional sobre Defesa Cibernética**, v. 55, n. 61, 2019. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=8054598&ts=1594004298782&disposition=inline. Acesso em: 1 out. 2023.

_____, Secretaria de Comunicação Social. **O que é a Política Nacional de**

Cibersegurança, marco no combate aos crimes virtuais, 2023a. Disponível em: https://www.gov.br/secom/pt-br/fatos/brasil-contra-fake/noticias/2023/3/o-que-e-a-politica-nacional-de-ciberseguranca-marco-no-combate-aos-crimes-virtuais#:~:text=A cibersegurança%2C ou segurança cibernética,usuários ou interromper processos empresariais. Acesso em: 22 fev. 2024.

_____, Secretaria-Geral da Presidência da República -. **Decreto nº 7.538**, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/decreto/d7538.htm#textoimpressao. Acesso em: 27 fev. 2024.

_____, Secretaria-Geral da Presidência da República -. **DECRETO Nº 7.682**, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Decreto/D7682.htm#art1. Acesso em: 14 out. 2023.

_____, Secretaria-Geral da Presidência da República. **Decreto nº 10.222 - Estratégia Nacional de Segurança Cibernética,** 2020b. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/decretos-federais/decreto-no-10-222-de-5-de-fevereiro-de-2020#:~:text=Aprova%20a%20Estrat%C3%A9gia%20Nacional%20de%20Seguran%C3%A7a%20Cibern%C3%A9tica.&text=Aprova%20a%20Estrat%C3%A9gia%20Nacional%20de%20Seguran%C3%A7a%20Cibern%C3%A9tica.,-Servi%C3%A7os. Acesso em: 9 out. 2023.

_____, TCU. **Cinco controles de segurança cibernética para ontem**, 2022h. Disponível em: https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/fiscalizacoes/. Acesso em: 5 dez. 2023.

_____ TCU. **Controles de Segurança Cibernética**, 2022g. Disponível em: https://portal.tcu.gov.br/data/files/E8/F0/BD/72/7D8A2810B4FE0FF7E18818A8/Ficha Sintese - 5 Controles de Seguranca Cibernetica.pdf. Acesso em: 23 dez. 2023.

_____ TCU. **Lista de Alto Risco da Administração Pública Federal 2022**, 2022e. Disponível em: https://sites.tcu.gov.br/listadealtorisco/seguranca_da_informacao_e_seguranca_cibernetica.html. Acesso em: 27 nov. 2023.

BRITO, Paulo. **Mercenários no mundo digital**, 2013. Disponível em: https://www.cisoadvisor.com.br/mercenarios-no-mundo-digital/. Acesso em: 15 fev.

2024.

BROAD, William J.; MARKOFF, John; SANGER, David E. **Israeli Test on Worm Called Crucial in Iran Nuclear Delay**. The New York Times, 2011. Disponível em: https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html. Acesso em: 23 dez. 2023.

BROWN, Christopher. **Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of North Korea**. Naval Postgraduate School, 2004. Disponível em: https://apps.dtic.mil/sti/pdfs/ADA427292.pdf. Acesso em: 11 nov. 2023.

BURTON, Chris. **Por que a Copa das Confederações não é mais disputada?**, 2022 Disponível em: https://www.goal.com/br/not%C3%ADcias/por-que-a-copa-das-confederacoes-nao-e-mais-disputada/bltc39f7dc2393dfcc8. Acesso em: 29 mar. 2024

BUXTON, Oliver. **Stuxnet: o que é e como funciona?**, 2022. Disponível em: https://www.avast.com/pt-br/c-stuxnet. Acesso em: 22 nov. 2023.

BYMAN, Daniel L. **Comparing Al Qaeda and ISIS: Different goals, different targets**. Brookings, 2015. Disponível em: https://www.brookings.edu/testimonies/comparing-al-qaeda-and-isis-different-goals-different-targets/? Acesso em: 24 out. 2023.

CAILLIAU, Robert. **Twenty years of a free and open www**. CERN Accelerating science, 2013. Disponível em: https://home.cern/news/opinion/computing/twenty-years-free-and-open-www. Acesso em: 19 out. 2023.

CAMBRIDGE. **Definição de cyberspace do Cambridge Advanced Learner's Dictionary & Thesaurus © Cambridge University Press**, 2022. Disponível em: https://dictionary.cambridge.org/pt/dicionario/ingles/cyberspace. Acesso em: 23 dez. 2023.

CAMPOS, João Pedroso de. **O partido é o poder**. Revista Veja, 2017. Disponível em: https://veja.abril.com.br/revista-veja/o-partido-e-o-poder. Acesso em: 24 fev. 2024.

CARDI, Marilza de Lourdes. **Evolução da Computação no Brasil e a sua relação com fatos internacionais**. Universidade Federal de Santa Catarina, 2002. Disponível em: https://repositorio.ufsc.br/xmlui/handle/123456789/84366. Acesso em: 22 nov.

2023.

CARDI, Marilza de Lourdes; BARRETO, Jorge Muniz. **Primórdios da Computação no Brasil**. Medellin: 2012. Disponível em: https://www.cos.ufrj.br/shialc/2012/content/docs/shialc_2/clei2012_submission_126.pdf. Acesso em: 16 fev. 2024.

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A trajetória da Internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança.** 2006. 239 f. COPPE/UFRJ, 2006. Disponível em: https://www.researchgate.net/profile/Marcelo-Carvalho-13/publication/268809917_A_TRAJETORIA_DA_INTERNET_NO_BRASIL_DO_SURGIMENTO_DAS_REDES_DE_COMPUTADORES_A_INSTITUICAO_DOS_MECANISMOS_DE_GOVERNANCA/links/54774a430cf2a961e4825bd4/A-TRAJETORIA-DA-INTERNET-NO.

CBN. **Governo faz contra-ataque cibernético para evitar ação de hackers no período da Copa**, 2014. Disponível em: https://cbn.globoradio.globo.com/grandescoberturas/copa-2014/2014/05/15/GOVERNO-FAZ-CONTRA-ATAQUE-CIBERNETICO-PARA-EVITAR-ACAO-DE-HACKERS-NO-PERIODO-DA-COPA.htm. Acesso em: 17 jan. 2024.

CERF, Vinton. **Internet Society**, 1994. Disponível em: https://web.archive.org/web/20160402062153/http://www.internetsociety.org/what-we-do/grants-and-awards/awards/postel-service-award/photo-gallery. Acesso em: 21 fev. 2024.

CERT.BR. **CERT.br registra aumento de ataques de negação de serviço em 2016**, 2017. Disponível em: https://nic.br/noticia/releases/cert-br-registra-aumento-de-ataques-de-negacao-de-servico-em-2016/. Acesso em: 9 out. 2023.

_____. **Códigos Maliciosos**, 2023. Disponível em: https://cartilha.cert.br/fasciculos/codigos-maliciosos/fasciculo-codigos-maliciosos.pdf. Acesso em: 18 fev. 2024.

_____. **Incidentes Notificados ao CERT.br,** 2024. Disponível em: https://stats.cert.br/incidentes/. Acesso em: 20 fev. 2024.

CERTEAU, Michel de. **A escrita da história.** Rio de Janeiro: Forense Universitária, 1982.

CGI.BR. **História do CGI.br**, [*s. d.*]. Disponível em: https://www.cgi.br/historicos/. Acesso em: 23 dez. 2023.

CHAI, Wesley; ROSENCRANCE, Linda. **Definition hacker**, 2021. Disponível em: https://www.techtarget.com/searchsecurity/definition/hacker. Acesso em: 16 jan. 2024.

CHAPARRO, Nixon Edier VARGAS. **La cibergeopolítica de China: un interés estratégico de Estado.** Revista científica Estudios en Seguridad y Defensa, 2022. Disponível em: https://esdegrevistas.edu.co/index.php/resd/article/view/328/525. Acesso em: 19 nov. 2023.

CHARTIER, Roger. **Os desafios da escrita**. Fundação Editora UNESP, São Paulo – SP, 2002.

CHEN, Xuechen; YANG, Yifan. **Contesting Western and Non-Western Approaches to Global Cyber Governance beyond Westlessness Contesting Western and Non-Western Approaches to Global Cyber Governance beyond Westlessness**, 2022. Disponível em: https://doi.org/10.1080/03932729.2022.2101231. Acesso em: 17 jan. 2024.

CHIASSON, Julien Lauzon. **Un cadre stratégique des opérations d'information de la Russie**. École nationale d'administration publique, 2019. Disponível em: https://espace.enap.ca/id/eprint/191/1/032321032.pdf. Acesso em: 19 out. 2023.

CIA.GOV. **RUSSIA**. *In*: THE WORLD FACTBOOK, 2023. Disponível em: https://www.cia.gov/the-world-factbook/countries/russia/#geography. Acesso em: 21 jan. 2024.

CISO. **Estônia registra pior incidente cibernético desde 2007**, 2022. Disponível em: https://www.cisoadvisor.com.br/estonia-sofre-pior-ataque-cibernetico-desde-2007/. Acesso em: 27 fev. 2024.

CISO ADVISOR. **Orçamento dos EUA para ciberdefesa alcança US$ 9,8 bilhões**. CISO Advisor, 2020. Disponível em: https://www.cisoadvisor.com.br/orcamento-dos-eua-para-ciberdefesa-alcanca-us-98-bilhoes/. Acesso em: 23 jan. 2024.

CLARKE, Richard A.; KNAKE, Robert K. **Guerra Cibernética - A próxima ameaça**

à Segurança e o que fazer a respeito. 1ªed.: Brasport Livros e Multimídia Ltda, 2015.

CLOUDFLARE. **O que é uma botnet?**, 2023. Disponível em: https://www.cloudflare.com/pt-br/learning/ddos/what-is-a-ddos-botnet/. Acesso em: 11 nov. 2023.

COB. **Rio 2016**, 2016. Disponível em: https://www.cob.org.br/pt/cob/time-brasil/brasil-nos-jogos/participacoes/rio-2016. Acesso em: 16 jan. 2024.

COLLI, Eduardo. **Universo olímpico - Uma enciclopédia das Olimpíadas**. 1. ed. São Paulo: Códex, 2004.

COLLINS, Sean; MCCOMBIE, Stephen. **Stuxnet: the emergence of a new cyber weapon and its implications**. Journal of Policing, Intelligence and Counter Terrorism, v. 7, n. 1, p. 80–91, 2012. Disponível em: http://www.tandfonline.com/action/showCitFormats?doi=10.1080/18335330.2012.653198. Acesso em: 19 out. 2023.

COMUNIDADE HARDWARE. **VIII Conferência Internacional de Perícias em Crimes Cibernéticos (ICCyber 2011)**, 2011. Disponível em: https://www.hardware.com.br/comunidade/viii-conferencia/1151523/. Acesso em: 5 out. 2023.

COPELAND, Jack B. **The Modern History of Computing**. Stanford Encyclopedia of Philosophy, 2006. Disponível em: https://plato.stanford.edu/entries/computing-history/. Acesso em: 16 fev. 2024.

CORERA, Gordon. **How France's TV5 was almost destroyed by "Russian hackers"**. BBC.com, 2016. Disponível em: https://www.bbc.com/news/technology-37590375. Acesso em: 28 dez. 2023.

COSSETTI, Melissa Cruz. O que é um backbone?. **Tecnoblog**, 2023. Disponível em: https://tecnoblog.net/responde/o-que-e-um-backbone/. Acesso em: 16 jan. 2024.

COSTA, Matheus Bigogno. **O que é DNS? | Trocá-lo pode ser a solução**, 2022. Disponível em: https://canaltech.com.br/internet/o-que-e-dns/. Acesso em: 5 out. 2023.

COSTA, Augusto Infanti Ribeiro da; CARDOSO, Helena Vieira; MEDINA, Patrick James. **Na Rede Social: Os movimentos sociais na atualidade**. Revista do Curso de Ciências Sociais da UFSC, 2013. Disponível em:

https://cienciassociais.ufsc.br/files/2015/03/Texto-14-Na-Rede-Social.pdf. Acesso em: 11 nov. 2023.

CPB. **Jogos Paralímpicos Rio 2016 quebram recordes de audiência**. Comitê Paralímpico Brasileiro, 2017. Disponível em: https://cpb.org.br/noticias/jogos-paralimpicos-rio-2016-quebram-recordes-de-audiencia/. Acesso em: 22 nov. 2023.

CRUZ VERMELHA. **O que é o direito internacional humanitário?**, 1998. Disponível em: https://www.icrc.org/pt/doc/resources/documents/misc/5tndf7.htm. Acesso em: 20 nov. 2023.

DAMIEN MCGUINNESS. **How a cyber attack transformed Estonia**. BBC News, 2017. Disponível em: https://www.bbc.com/news/39655415. Acesso em: 16 jan. 2024.

DANTAS, Vera. **Guerrilha tecnológica: a verdadeira história da política nacional de informática**. Rio de Janeiro, RJ: Livros Técnicos e Científicos, 1988.

DARAKTCHIEV, Ivan. **Nomenklaturocracy, or what exactly was Orwell right about**, 2013. Disponível em: https://www.academia.edu/4439386/Nomenklaturocracy_or_what_exactly_was_Orwell_right_about. Acesso em: 14 out. 2023.

DARPA. **About DARPA**, 2024. Disponível em: https://www.darpa.mil/about-us/about-darpa. Acesso em: 15 fev. 2024.

DAVENPORT, Kelsey. **Timeline of Nuclear Diplomacy With Iran, 1967-2023**. Arms Control Association, 2023. Disponível em: https://www.armscontrol.org/factsheets/Timeline-of-Nuclear-Diplomacy-With-Iran. Acesso em: 15 fev. 2024.

DAVIS, Joshua. **Hackers Take Down the Most Wired Country in Europe**, 2007. Disponível em: https://www.wired.com/2007/08/ff-estonia/?currentPage=all. Acesso em: 19 out. 2023.

DEMARTINI, Felipe. **Ataque de ransomware paralisa 16 hospitais nos EUA**. Canaltech, 2023. Disponível em: https://canaltech.com.br/seguranca/ataque-de-ransomware-paralisa-16-hospitais-nos-eua-258740/. Acesso em: 9 mar. 2024.

DEMARTINI, Felipe. **Governo brasileiro sofre novo ataque de ransomware**. **Canaltech**, 2022. Disponível em: https://canaltech.com.br/seguranca/governo-

brasileiro-sofre-novo-ataque-de-ransomware-224259/. Acesso em: 27 fev. 2024.

DEMENTSHUK, Márcia; HENRIQUES, Percival. **Pássaros Voam em Bando: a história da Internet do século XVIII ao século XXI**. 1ªed. João Pessoa: Editora ANID, 2019.

DORES, Renan da Silva. **O que é RFID?**, 2022. Disponível em: https://canaltech.com.br/hardware/o-que-e-rfid-947/. Acesso em: 15 fev. 2024.

E-ESTONIA. **X-ROAD**, 2023. Disponível em: https://e-estonia.com/solutions/interoperability-services/x-road/. Acesso em: 15 fev. 2024.

ECONOMIST, THE. **George Bush and the axis of evil**. The Economist, 2002. Disponível em: https://www.economist.com/leaders/2002/01/31/george-bush-and-the-axis-of-evil. Acesso em: 3 nov. 2023.

EHALA, Martin. **The bronze soldier: Identity threat and maintenance in Estonia**. Journal of Baltic Studies, v. 40, p. 139–158, 2009. Disponível em: https://www.tandfonline.com/doi/full/10.1080/01629770902722294. Acesso em: 22 nov. 2023.

ESTADOS UNIDOS, Library of Congress. **Estonia, Latvia, and Lithuania: country studies**. 1. ed. Washington - DC: Area handbook series, 1996.

_____. **DOD Dictionary of Military and Associated Terms**, 2021. Disponível em: https://irp.fas.org/doddir/dod/dictionary.pdf. Acesso em: 30 jan. 2024.

_____, NSA. **Our Mission**, 2024. Disponível em: https://www.nsa.gov/. Acesso em: 15 fev. 2024.

ESTONIA. **Estonia is the world's first country to also function as a digital service**, 2023. Disponível em: https://estonia.ee/enter/. Acesso em: 21 jan. 2024.

EUROPEU, Parlamento. **Resolução do Parlamento Europeu, de 15 de fevereiro de 2023, sobre a situação do antigo Presidente da Geórgia, Mikheil Saakashvili,** 2023. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0046_PT.html. Acesso em: 15 fev. 2024.

EY, Agência. **Brasil melhora na digitalização do governo, mas confiança da população ainda é baixa**, 2023. Disponível em: https://www.ey.com/pt_br/agencia-

ey/noticias/brasil-melhora-digitalizacao-governo-mas-confianca-populacao-baixa#:~:text=O Brasil é o sexto,) e Argentina (41ª). Acesso em: 15 jan. 2024.

FALLIERE, Nicolas; MURCU, Liam O.; CHIEN, Eric. **W32. stuxnet dossier,** 2011. Disponível em: https://pax0r.com/hh/stuxnet/Symantec-Stuxnet-Update-Feb-2011.pdf. Acesso em: 11 nov. 2023.

FAN, Ricardo. **Órgãos de segurança montam estrutura para combater ataques cibernéticos na Copa do Mundo**. O Defesanet, 2014. Disponível em: https://www.defesanet.com.br/pensamento/orgaos-de-seguranca-montam-estrutura-para-combater-ataques-ciberneticos-na-copa-do-mundo/. Acesso em: 18 nov. 2023.

FAPESP. **A instituição**, 2023. Disponível em: https://fapesp.br/sobre/. Acesso em: 23 dez. 2023.

FARWELL, James; RAFAL ROHOZINSKI. **Stuxnet and the future of cyber war**. Survival, v. 53, n. 1, p. 23–40, 2011. Disponível em: https://courses.cs.duke.edu/common/compsci092/papers/cyberwar/stuxnet2.pdf. Acesso em: 15 fev. 2024.

FERNANDES, Cleonice Terezinha. **A Construção do Conceito de Número e o Pré-Soroban**. Brasília: Ministério da Educação, 2006. Disponível em: http://www.dominiopublico.gov.br/download/texto/me4619.pdf. Acesso em: 21 jan. 2024.

FERREIRA, Tamires. **Brasil está entre os cinco países que mais sofrem ataques ransomware.** Olhar Digital, 2022. Disponível em: https://olhardigital.com.br/2022/09/11/seguranca/brasil-esta-entre-os-cinco-paises-que-mais-sofrem-ataques-ransomware/. Acesso em: 16 fev. 2024.

FERREIRA, Jorge. **URSS: Mito, utopia e história**. Tempo, Rio de Janeiro, p. 75–103, 1998. Disponível em: https://beneweb.com.br/resources/URSS Mito utopia e história.pdf. Acesso em: 16 fev. 2024.

FIGUEIREDO, Nice. **Legislação de informática no Brasil; desenvolvimento e debates**. Revista de Biblioteconomia de Brasília, v. 14, n. n.2, p. 287–297, 1986. Disponível em: https://periodicos.unb.br/index.php/rbbsb/article/view/41686. Acesso em: 16 fev. 2024.

FOLHA. **Ministro nega que ataque hacker possa ter causado apagão**. **Folha cotidiano**, 2009b. Disponível em: https://m.folha.uol.com.br/cotidiano/2009/11/650656-ministro-nega-que-ataque-hacker-possa-ter-causado-apagao.shtml?cmpid=menupe. Acesso em: 14 out. 2023.

_____. **Para EUA, hacker causou apagão no Brasil**. Folha de São Paulo, 2009a. Disponível em: https://www1.folha.uol.com.br/fsp/dinheiro/fi0811200905.htm. Acesso em: 23 dez. 2023.

FONSECA FILHO, Cléuzio. **História da Computação - O caminho do pensamento e da tecnologia**. Porto Alegre - RS: EDIPUCRS, 2007. Disponível em: https://www.academia.edu/7969231/História_da_Computação_o_caminho_do_pensamento_e_da_tecnologia. Acesso em: 16 fev. 2024.

FORTINET. **Fortinet relata que a América Latina foi alvo de mais de 360 bilhões de tentativas de ataques cibernéticos em 2022**, 2023. Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2023/fortiguard-labs-reports-destructive-wiper-malware-increases-over-50-percent. Acesso em: 16 jan. 2024.

FREIRE, Maria Raquel; SIMÃO, Licínia. **A Rússia e o Cáucaso do Sul: das relações neocoloniais à realpolitik no" estrangeiro próximo**. A Política Externa Russa no Espaço Euro-Atlântico: Dinâmicas de cooperação e competição num espaço alargado, p. 85–112, 2014. Disponível em: http://hdl.handle.net/10316.2/31902. Acesso em: 8 out. 2023.

G1. **Ativistas ameaçam atacar sites da Copa do Mundo**, 2014. Disponível em: https://g1.globo.com/tecnologia/noticia/2014/02/ativistas-ameacam-atacar-sites-da-copa-do-mundo.html. Acesso em: 16 fev. 2024.

____. **“Bombardeio virtual” de hackers deu início ao ataque contra a Geórgia**, 2008. Disponível em: https://g1.globo.com/Noticias/Tecnologia/0,,MUL729549-6174,00-BOMBARDEIO+VIRTUAL+DE+HACKERS+DEU+INICIO+AO+ATAQUE+CONTRA+A+GEORGIA.html. Acesso em: 15 fev. 2024.

_____. **Segurança da Rio+20 tem equipes para conter ataques cibernéticos e terrorismo**, 2012. Disponível em:

https://g1.globo.com/mundo/noticia/2012/06/seguranca-da-rio20-tem-equipes-para-conter-ataques-ciberneticos-e-terrorismo.html. Acesso em: 16 jan. 2024.

GCI, Global Cybersecurity Index. **GCI results: Score and rankings**. ITU Publications, 2020. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf. Acesso em: 27 fev. 2024.

GEORGIA, National Statistics Office of. **Demographic Situation In Georgia 2022**, 2023. Disponível em: https://www.geostat.ge/en/single-archive/3396. Acesso em: 19 fev. 2024.

GIELOW, Igor. **Guerra que fez de Putin vilão também consolidou seu poder**. Folha de São Paulo, 2018. Disponível em: https://www1.folha.uol.com.br/mundo/2018/08/guerra-que-fez-de-putin-vilao-tambem-consolidou-seu-poder.shtml. Acesso em: 20 fev. 2024.

GILES, Keir. **Handbook of Russian Information Warfare**, 2016. Disponível em: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/NDC fm_9.pdf. Acesso em: 16 jan. 2024.

_____. **Information Troops – a Russian Cyber Command?**. Conflict Studies Research Centre, Oxford, UK. 3rd Internacional Conference on Cyber Conflict, 2011. Disponível em: https://www.ccdcoe.org/uploads/2018/10/InformationTroopsARussianCyberCommand-Giles.pdf. Acesso em: 12 fev. 2024.

GLOBO. **Eleição do Rio como sede dos Jogos de 2016**. Memória Globo, 2021. Disponível em: https://memoriaglobo.globo.com/jornalismo/coberturas/eleicao-do-rio-como-sede-dos-jogos-de-2016/noticia/eleicao-do-rio-como-sede-dos-jogos-de-2016.ghtml. Acesso em: 7 jan. 2024.

GOFF, Jacques Le. **História e Memória**. Campinas, SP: 1990. Disponível em: https://edisciplinas.usp.br/pluginfile.php/4594598/mod_resource/content/1/LE_GOFF_HistoriaEMemoria.pdf.

GOGONI, Ronaldo. **O que é 5G?**, 2019. Disponível em: https://tecnoblog.net/responde/o-que-e-5g/. Acesso em: 22 nov. 2023.

GOMES, Helton Simões. **Exército monitorará redes sociais durante visita do Papa e**

Copa de 2014. G1 Tecnologia e Games, 2013. Disponível em: https://g1.globo.com/tecnologia/noticia/2013/07/exercito-monitorara-redes-sociais-durante-visita-do-papa-e-copa-de-2014.html. Acesso em: 5 dez. 2023.

_____. **Sociedade digital**. UOL, 2023. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2023/10/18/por-que-a-estonia-pais-mais-digital-do-mundo-esta-atras-de-brasileiros.htm. Acesso em: 21 fev. 2024.

GOULART, Josette. **Empresa dona do maior oleoduto americano cede e paga resgate a hackers**. VEJA, 2021. Disponível em: https://veja.abril.com.br/coluna/radar-economico/empresa-dona-do-maior-oleoduto-americano-cede-e-paga-resgate-a-hackers/. Acesso em: 15 fev. 2024.

GRAHAM, Bob. **World War II's first victim**. The Telegraph, 2009. Disponível em: https://web.archive.org/web/20120314190818/http:/www.telegraph.co.uk/history/world-war-two/6106566/World-War-IIs-first-victim.html. Acesso em: 27 fev. 2024.

GREENE, David. **Russian Minority Struggles In Post-Soviet Estonia**. NPR, 2010. Disponível em: https://www.npr.org/templates/story/story.php?storyId=129333023. Acesso em: 9 out. 2023.

GUGIK, Gabriel. **A História dos computadores e da computação**. Tecmundo, 2009. Disponível em: https://iow.unirg.edu.br/public/profarqs/2804/0272700/1.A_Historia_dos_computadores_e_da_computacao_-_imprimir.pdf. Acesso em: 14 out. 2023.

HADDICK, Robert. **This week at war: Lessons from cyberwar I – How Russia pioneered the use of cyberattacks as military tactic**. Foreignpolicy, 2018. Disponível em: https://blogs.ubc.ca/security/files/2014/08/This-Week-at-War_-Lessons-from-Cyberwar-I.pdf. Acesso em: 5 out. 2023.

HAFNER, Katie; LYON, Matthew. **Where wizards stay up late: The origins of the Internet**. 1ªed. Nova York: Simon and Schuster, 1998.

HANDLER, Sephenie Gosnell. **New cyber face of battle: developing a legal approach to accommodate emerging trends in warfare.** Stan. J. Int'l L, v. 48, 2012. Disponível em: https://heinonline.org/HOL/LandingPage?handle=hein.journals/stanit48&div=10&id=&page=. Acesso em: 9 out. 2023.

HEART, F. E. *et al.* **The interface message processor for the ARPA computer network**. Proceedings of the May 5-7, 1970, spring joint computer conference, p. 551–567, 1970. Disponível em: https://dl.acm.org/doi/pdf/10.1145/1476936.1477021. Acesso em: 9 out. 2023.

HELENA, Silva. **Rastro de Cobra**. Rio de Janeiro, RJ: Caio Domingues & Associados Publicidade Ltda, 1984.

HELLER, Nathan. **Estonia, the digital republic**. The New Yorker, 2017. Disponível em: https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic. Acesso em: 5 dez. 2023.

HERÉDIA, Thais. **Ataque revela fragilidade na estrutura energética dos EUA**, 2021. Disponível em: https://www.cnnbrasil.com.br/economia/ataque-revela-fragilidade-na-estrutura-energetica-dos-eua-diz-analista/. Acesso em: 18 fev. 2024.

HOBSBAWM, Eric. **Era dos extremos: o breve século XX**. 2ªed. São Paulo: Companhia das Letras, 1995.

HOEPERS, Cristine. **Atuação do CERT.br e Lições Aprendidas no Tratamento de Incidentes na Rio 2016**. CERT.br, 2017. Disponível em: https://www.cert.br/docs/palestras/certbr-comdciber2017.pdf. Acesso em: 16 fev. 2024.

IFRAH, Georges. **História Universal dos Algarismos**. Nova Fronteira, 1997.

INOHARA, André. **Brasil monitora ameaças cibernéticas em função dos grandes eventos que sediará nos próximos anos**, 2011. Disponível em: https://webcache.googleusercontent.com/search?q=cache:vBrFwUs2pF4J:https://www.amcham.com.br/noticias/juridico/brasil-monitora-ameacas-ciberneticas-em-funcao-dos-grandes-eventos-que-sediara-nos-proximos-anos&hl=pt-BR&gl=br. Acesso em: 22 nov. 2023.

ITU-T. **Overview of cybersecurity**. International Telecommunication Union, 2008. Disponível em: https://www.itu.int/rec/T-REC-X.1205-200804-I. Acesso em: 22 fev. 2024.

KASPERSKY. **O que é o Rootkit – Definição e Explicação**, 2023c. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-rootkit. Acesso em: 30 jan. 2024.

_____. **O que é cibersegurança?** 2024a. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-cyber-security. Acesso em: 22 mar. 2024.

_____. **O que é spear phishing? Definição e riscos**, 2024b. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/spear-phishing. Acesso em: 22 mar. 2024.

_____. **O que é um ataque de dia zero? – Definição e explicação**, 2023d. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/zero-day-exploit. Acesso em: 19 jan. 2024.

_____. **O que são ataques de DDoS?**, 2023b. Disponível em: https://www.kaspersky.com.br/resource-center/threats/ddos-attacks. Acesso em: 10 jan. 2024.

_____. **O que são bots? - Definição e Explicação**, 2023a. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-are-bots. Acesso em: 20 fev. 2024.

KEATING, Maj Kenneth C. **U.S Army Russian Institute – Student research report: Maskirovka – The Soviet System of Camouflage**. Garmisch, 1981. Disponível em: https://apps.dtic.mil/dtic/tr/fulltext/u2/a112903.pdf. Acesso em: 3 nov. 2023.

KENYON, Henry. **The network of our times.** DARPA Defense Advanced Research Projects Agency, 2018. Disponível em: https://www.darpa.mil/attachments/DARAPA60_publication-no-ads.pdf. Acesso em: 22 nov. 2023.

KHINKULOVA, Kateryna; IVSHINA, Olga. **Morre Mikhail Gorbachev: 5 razões pelas quais a União Soviética entrou em colapso**. BBC Rússia, 2022. Disponível em: https://www.bbc.com/portuguese/internacional-62731864. Acesso em: 23 dez. 2023.

KING, Charles. **Clarity in the Caucasus?** Foreign Affairs, 2009. Disponível em: https://www.foreignaffairs.com/articles/russia-fsu/2009-10-11/clarity-caucasus. Acesso em: 22 nov. 2023.

KNORR-EVANS, Maite. **What is a false flag operation?**. **US News**, 2022. Disponível em: https://en.as.com/en/2022/02/18/latest_news/1645138852_316937.html. Acesso

em: 14 out. 2023.

KONCHINSKI, Vinicius. **Ataque hacker tira do ar site governamental sobre a Copa do Mundo.** UOL, 2013. Disponível em: https://copadomundo.uol.com.br/noticias/redacao/2013/06/18/ataque-hacker-tira-do-ar-site-governamental-sobre-a-copa-do-mundo.htm. Acesso em: 16 fev. 2024.

KORNS, Stephen W.; KASTENBERG, Joshua E. **Georgia's cyber left hook**. Parameters, 2008. Disponível em: https://apps.dtic.mil/sti/tr/pdf/ADA636632.pdf. Acesso em: 3 nov. 2023.

KOVACS, Leandro. **O que é um firewall? [E a diferença para um antivírus]**, 2021. Disponível em: https://tecnoblog.net/responde/o-que-e-um-firewall-e-a-diferenca-para-um-antivirus/. Acesso em: 22 nov. 2023.

_____. **Qual a origem e história do grupo Anonymous?**. Tecnoblog, 2023. Disponível em: https://tecnoblog.net/responde/qual-a-origem-e-historia-do-grupo-anonymous/. Acesso em: 16 fev. 2024.

KREMER, An-Frederik; MULLER, Benedikt. **Cyberspace and International Relations**. Berlim: Springer Berlin Heidelberg, 2014. Disponível em: https://link.springer.com/10.1007/978-3-642-37481-4.

KUEHL, Daniel T. **From Cyberspace to Cyberpower: Defining the Problem**, v. 30, 2009. Disponível em: https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210. Acesso em: 27 jan. 2024.

KUVIATKOSKI, Carol. **Spin-off: o que é e como usar para alavancar o seu negócio**. **Ideia no ar**, 2022. Disponível em: https://www.ideianoar.com.br/spin-off/. Acesso em: 27 fev. 2024.

LÉVY, Pierre. **A emergência do cyberspace e as mutações culturais**, 1994. Disponível em: https://www.nescon.medicina.ufmg.br/biblioteca/imagem/2514.pdf. Acesso em: 30 jan. 2024.

_____. **Cibercultura.** São Paulo: Ed. 34**,** 1999.

LIBICKI, Martin C. **Cyberdeterrence and Cyberwar**, 2010. ISSN 1089-7798. Disponível em: http://www.rand.org/pubs/research_briefs/RB9539.html.

LICKLIDER, Joseph Carl Robnett; CLARK, Welden E. **On-line man-computer communication.** Proceedings of the May 1-3, 1962, spring joint computer conference, p. 113–128, 1962. Disponível em: https://dl.acm.org/doi/10.1145/1460833.1460847. Acesso em: 16 jan. 2024.

LOBO, Ana Paula. **Governo define política de segurança cibernética, mas adia agência nacional**. Convergência Digital, 2023. Disponível em: https://www.convergenciadigital.com.br/Seguranca/Governo-define-politica-de-seguranca-cibernetica%2C-mas-adia-agencia-nacional-65024.html?UserActiveTemplate=mobile. Acesso em: 21 fev. 2024

LORENZO, Alessandro Di. **Brasil é o segundo maior alvo de crimes cibernéticos na América Latina.** Olhar Digital, 2024. Disponível em: https://olhardigital.com.br/2024/02/02/seguranca/brasil-e-o-segundo-maior-alvo-de-crimes-ciberneticos-na-america-latina/. Acesso em: 27 fev. 2024.

MACEDO, Joyce. **Botnets: descubra se o seu computador faz parte de uma e saiba como se proteger**, 2013. Disponível em: https://arquivo.canaltech.com.br/seguranca/Botnets-descubra-se-o-seu-computador-faz-parte-de-uma-e-saiba-como-se-proteger/. Acesso em: 16 jan. 2024.

MACFARLANE, Neil S. **The 'R'in BRICs: is Russia an emerging power?** International affairs, v. 82, n. 1, p. 41–57, 2006. Disponível em: https://ccs.ukzn.ac.za/files/the R in BRICS - is Russia an emerging power.pdf. Acesso em: 22 nov. 2023.

MACHADO, José Alberto S. **Ativismo em rede e conexões identitárias: novas perspectivas para os movimentos sociais.** Sociologias, p. 248–285, 2007. Disponível em: https://www.scielo.br/j/soc/a/JKWntC6dkPCjpRXtXfFzYzk/?lang=pt&format=pdf. Acesso em: 24 out. 2023.

MAKARYCHEV, Andrey S. A Rússia, a Europa e o legado de 1989. **Relações Internacionais**, v. 23, 2009. Disponível em: https://ipri.unl.pt/images/publicacoes/revista_ri/pdf/ri23/n23a04.pdf. Acesso em: 19 nov. 2023.

MARCELINO, Gileno Fernandes. **A indústria nacional de computadores**. Revista de Administração, v. 18, p. 90–95, 1983.

MARTINS, Paula. **Da Cibersegurança à ciberguerra – O desenvolvimento de políticas de vigilância no Brasil.** Artigo 19, 2016. Disponível em: https://artigo19.org/wp-content/blogs.dir/24/files/2016/03/Da-Cibersegurança-à-Ciberguerra-WEB.pdf. Acesso em: 24 out. 2023.

MARTINS, Elaine. **O que é TCP/IP?**, 2012. Disponível em: https://www.tecmundo.com.br/o-que-e/780-o-que-e-tcp-ip-.htm. Acesso em: 29 fev. 2024.

MATSUURA, Sérgio. **Pesquisador reconstitui o dia, há 50 anos, em que criou a internet**. O Globo Economia, 2019. Disponível em: https://oglobo.globo.com/economia/tecnologia/pesquisador-reconstitui-dia-ha-50-anos-em-que-criou-internet-24045049. Acesso em: 18 nov. 2023.

MAURER, Tim. **Cyber Mercenaries**. Cambridge: Cambridge University Press, 2018. Disponível em: https://www.cambridge.org/core/product/identifier/9781316422724/type/book. Acesso em: 23 dez. 2023.

MAZNOVA, Snizhana. **Alfabeto Russo**, 2010. Disponível em: https://www.cursorusso.com.br/alfabeto-russo/. Acesso em: 15 fev. 2024.

MELLO, Michele de. **9 de maio de 1945: o Dia da Vitória da Rússia contra a Alemanha nazista de Hitler**. Brasil de Fato, 2021. Disponível em: https://www.brasildefato.com.br/2021/05/09/9-de-maio-de-1945-o-dia-da-vitoria-da-russia-contra-a-alemanha-nazista-de-hitler. Acesso em: 16 fev. 2024.

MELO, João Ozório de. **Automação em julgamentos chega aos tribunais dos EUA e da Estônia**, 2023. Disponível em: https://www.conjur.com.br/2023-jan-24/automacao-julgamentos-chega-aos-tribunais-eua-estonia/#:~:text=Na Estônia%2C só podem contar,recorrer a um juiz humano. Acesso em: 15 fev. 2024.

MIELNICZUK, Fabiano. **O conflito entre Rússia e Geórgia: uma revisão histórica**. Estudos Internacionais: revista de relações internacionais da PUC Minas, p. 157–166, 2013. Disponível em: https://periodicos.pucminas.br/index.php/estudosinternacionais/article/view/6311/5790. Acesso em: 21 jan. 2024.

MILHAZES, José. **Dirigentes russos reconhecem crise tecnológica no país**, 2009.

Disponível em: https://darussia.blogspot.com/2009/07/dirigentes-russos-reconhecem-crise.html. Acesso em: 20 dez. 2023.

MORAES, Bruno. **Estratégia de Segurança Cibernética dos Jogos Rio 2016**. Linkedin, 2016. Disponível em: https://pt.linkedin.com/pulse/estratégia-de-segurança-cibernética-dos-jogos-rio-2016-bruno-moraes. Acesso em: 22 nov. 2023.

MORAES, Raquel de Almeida. **Informática educativa no Brasil: das origens à década de 1990**. 1. ed. Uberlândia: Navegando Publicações, 2016. Disponível em: https://www.editoranavegando.com/livro-raquel. Acesso em: 18 nov. 2023.

MORAES, Thiago Perez Bernardes de; SANTOS, Romer Mottinha. Charlie Hebdo: **Polémica, religião e o interesse dos usuários de Internet franceses**. **OpenEdition Journals,** v. 11, 2016. Disponível em: https://journals.openedition.org/cp/1193#tocto1n2. Acesso em: 19 nov. 2023.

MOREIRA, Pedro. **Conheça a trajetória do fundador do Wikileaks, Julian Assange**. Radio Agência, 2023. Disponível em: https://agenciabrasil.ebc.com.br/radioagencia-nacional/internacional/audio/2023-08/conheca-trajetoria-do-fundador-do-wikileaks-julian-assange. Acesso em: 16 jan. 2024.

MOREIRA, José de Alburquerque. **Informática: o mito Política Nacional de Informática**. Revista de Biblioteconomia de Brasília, v. 19, n. 1, p. 23–50, 1995. Disponível em: https://periodicos.unb.br/index.php/rbbsb/article/view/46356. Acesso em: 16 fev. 2024.

MOREIRA, Alexandre Santana *et al.* **Inovação em Defesa Cibernética Brasileira no contexto Sul-Americano**, v. 23, p. 87–104, 2014. Disponível em: https://periodicos.ufpe.br/revistas/politicahoje/article/view/3743. Acesso em: 16 fev. 2024.

MORIMOTO, Carlos E. **O ENIAC – A História da Informática**, 2011. Disponível em: https://www.hardware.com.br/guias/historia-informatica/eniac.html. Acesso em: 22 nov. 2023.

MUGGAH, Robert; THOMPSON, Nathan B. **Novos ataques do Anonymous no Rio marcam início dos jogos digitais**. El País, 2016. Disponível em: https://brasil.elpais.com/brasil/2016/08/15/opinion/1471267832_175141.html. Acesso em: 9 out. 2023.

MUNDO, Mapas del. **Grande detallado mapa político de Georgia, Abjasia y Osetia del Sur con carreteras, ferrocarriles, ciudades y aeropuertos**, 2024. Disponível em: https://www.mapas-del-mundo.net/mapas/asia/abjasia/grande-detallado-mapa-politico-de-georgia-abjasia-y-osetia-del-sur-con-carreteras-ferrocarriles-ciudades-y-aeropuertos.jpg. Acesso em: 19 fev. 2024.

NALIM, Carolina. **Brasil é o maior alvo de ataques cibernéticos na América Latina**. **Veja ranking**. O Globo Tecnologia, 2023. Acesso em: 10 jan. 2024.

NASCIMENTO, Anderson. **O que é ping?** Canaltech, 2014. Disponível em: https://canaltech.com.br/internet/o-que-e-ping/. Acesso em: 23 dez. 2023.

NEC. **Copa do Mundo: atenção aos ataques cibernéticos**, 2018. Disponível em: https://blog.nec.com.br/copa-do-mundo-atencao-aos-ataques-ciberneticos. Acesso em: 5 out. 2023.

NERY, Severino Motta Natuza. **PF prevê ataques cibernéticos em massa no dia de abertura da Copa.** Folha de São Paulo, 2014. Disponível em: https://m.folha.uol.com.br/mundo/2014/05/1460911-pf-preve-ataques-ciberneticos-em-massa-no-dia-de-abertura-da-copa.shtml. Acesso em: 19 nov. 2023.

NETTO, Irinêo Baptista. **Paradoxo russo**. Gazeta do Povo, 2011. Disponível em: https://www.gazetadopovo.com.br/mundo/paradoxo-russo-aqzgon438enc8m1berttejo7i/. Acesso em: 16 jan. 2024.

NORTON. **O que são bots?**, 2018. Disponível em: https://br.norton.com/blog/malware/what-are-bots. Acesso em: 15 fev. 2024.

OLIVEIRA, Pedro Ivo de. **Agência Brasil explica: entenda a deep web e a dark web.** Agência Brasil - EBC, 2020. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2020-09/agencia-brasil-explica-entenda-deep-web-e-dark-web. Acesso em: 24 out. 2023.

OLIVEIRA, Marcos de. Demi Getschko: **Um construtor da internet**. Pesquisa FAPESP, 2014. Disponível em: https://revistapesquisa.fapesp.br/demi-getschko-um-construtor-da-internet/. Acesso em: 22 nov. 2023.

OLIVEIRA, Marcos. **Nasce a internet**. Revista Fapesp, n. 180, p. 23–25, 2011. Disponível em: https://revistapesquisa.fapesp.br/folheie-a-ed-180/. Acesso em: 18 fev.

2024.

OLIVEIRA, José Carlos. **Olimpíadas 2016: a histórica conquista do Rio como sede olímpica**. Rádio Câmara, 2015. Disponível em: https://www.camara.leg.br/radio/programas/458862-olimpiadas-2016-a-historica-conquista-do-rio-como-sede-olimpica/. Acesso em: 18 nov. 2023.

OLIVEIRA, Marcos de. **Primórdios da rede**. Pesquisa FAPESP, 2011. Disponível em: https://revistapesquisa.fapesp.br/primórdios-da-rede_/#:~:text=O grupo do CPD da,Yale%2C no estado de Connecticut. Acesso em: 19 out. 2023.

ONU, Assembleia Geral da. **Declaração Universal dos Direitos Humanos**, 1948. Disponível em: https://www.oas.org/dil/port/1945 Carta das Nações Unidas.pdf. Acesso em: 22 nov. 2023.

____, Conselho de Segurança. **'Explosive' Growth of Digital Technologies Creating New Potential for Conflict, Disarmament Chief Tells Security Council in First-Ever Debate on Cyberthreats**, 2021. Disponível em: https://press.un.org/en/2021/sc14563.doc.htm. Acesso em: 22 nov. 2023.

____. **Resolution adopted by the General Assembly on 5 December 2018**, 2018. Disponível em: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/418/04/PDF/N1841804.pdf?OpenElement. Acesso em: 27 fev. 2024.

_____. **Rio +20 - Conferência das Nações Unidas sobre desenvolvimento sustentável**, 2012. Disponível em: https://www.acnur.org/fileadmin/Documentos/portugues/eventos/Rio_20_Futuro_que_queremos_guia.pdf?view=1. Acesso em: 16 fev. 2024.

OPAS. **OMS declara fim da Emergência de Saúde Pública de Importância Internacional referente à COVID-19**, 2023. Disponível em: https://www.paho.org/pt/noticias/5-5-2023-oms-declara-fim-da-emergencia-saude-publica-importancia-internacional-referente#:~:text=Brasília%2C 5 de maio de,) referente à COVID-19. Acesso em: 27 fev. 2024.

OXFORD, University of. **Sir Tim Berners-Lee joins Oxford's Department of Computer Science**, 2016. Disponível em: https://www.ox.ac.uk/news/2016-10-27-sir-tim-berners-lee-joins-oxfords-department-computer-science. Acesso em: 20 nov. 2023.

PEREYRA, D. **Mercenarios.** El Viejo Topo, 2007. Disponível em: https://books.google.com.br/books?id=WOk3xVvlNGUC. Acesso em: 9 mar. 2024.

PERKOVITCH, George; LEVITE, Ariel. **Understanding cyber conflict : 14 analogies**. Washington, DC: Georgetown University Press, 2017.

PINTO, Paulo Sousa. **A dissolução da URSS e formação da Comunidade de Estados Independentes**, 2017. Disponível em: https://ensina.rtp.pt/artigo/a-dissolucao-da-urss-e-formacao-da-comunidade-de-estados-independentes/. Acesso em: 11 nov. 2023.

PIRES, Raquel Lopes; DE AMORIM, Sara Raphaela Machado. **História digital e o ofício do historiador: Modos de ser e fazer no repositório da revista Pour l'ère nouvelle**. Holos, v. 8, p. 1-16, 2021. Disponível em: https://www2.ifrn.edu.br/ojs/index.php/HOLOS/article/download/11773/pdf/31581. Acesso em: 20 nov. 2023.

POULSEN, Kevin. **Report: Cyber Attacks Caused Power Outages in Brazil**. Wired, 2009. Disponível em: https://www.wired.com/2009/11/brazil/. Acesso em: 5 dez. 2023.

PRACIANO, Daniel. **Saiba como foram os primeiros passos do Brasil na internet antes da era comercial.** NIC.br, 2019. Disponível em: https://www.nic.br/noticia/na-midia/saiba-como-foram-os-primeiros-passos-do-brasil-na-internet-antes-da-era-comercial/. Acesso em: 23 dez. 2023.

PRADO, José L. Gómez Del. **Los nuevos mercenarios del siglo XXI**, 2014. Disponível em: https://www.fuhem.es/media/cdv/file/biblioteca/PDF Papeles/94/Nuevos_mercenarios_sXXI_ Gomezdel Prado.pdf. Acesso em: 26 out. 2023.

PRESSE, France. **Ex-presidente georgiano foi envenenado na prisão, afirmam médicos.** G1, 2022. Disponível em: https://g1.globo.com/mundo/noticia/2022/12/05/ex-presidente-georgiano-saakashvili-foi-envenenado-na-prisao-afirmam-medicos.ghtml. Acesso em: 20 nov. 2023.

RADWARE. **Killnet**, 2023. Disponível em: https://www.radware.com/cyberpedia/ddos-attacks/killnet/. Acesso em: 5 dez. 2023.

RAMINA, Larissa Liz Odreski. **O princípio da autodeterminação dos povos e seus paradoxos: a aplicação na guerra do Cáucaso de 2008**, 2010. Disponível em: http://www.publicadireito.com.br/conpedi/manaus/arquivos/anais/fortaleza/3336.pdf.

Acesso em: 2 jan. 2024.

RAMÍREZ, Juan David García. **El papel de los mercenarios en los conflictos internacionales: de la Grecia clásica a las compañías militares privadas de hoy**, v. 5, n. 8, p. 169–182, 2015. Disponível em: https://revistas.upb.edu.co/index.php/analecta/article/view/2506/2275. Acesso em: 26 out. 2023.

RAND. **50th Project Air Force 1946 – 1996,** 1996. Disponível em: https://www.rand.org/about/history.html. Acesso em: 24 out. 2023.

____. **A Brief History of RAND**, 2024. Disponível em: https://www.rand.org/about/history.html. Acesso em: 16 fev. 2024.

RANDIG, Rodrigo Wiese. **Guerra na Ossétia do Sul: a Geórgia como foco de conflito entre a Rússia e o Ocidente**. Meriadiano 47, 2008. Disponível em: https://web.archive.org/web/20090923105355/http://meridiano47.info:80/2008/08/31/guerra-na-ossetia-do-sul-a-georgia-como-foco-de-conflito-entre-a-russia-e-o-ocidente-por-rodrigo-wiese-randig/. Acesso em: 19 out. 2023.

RIBEIRO, Daniel. **Como funciona um roteador e saiba quais os tipos existentes**, 2013. Disponível em: https://www.techtudo.com.br/noticias/2013/05/como-funciona-um-roteador-e-saiba-quais-os-tipos-existentes.ghtml. Acesso em: 16 fev. 2024.

RIBEIRO, Luiz Felipe. **Criptomoedas: entenda o que são e como funcionam**, 2022. Disponível em: https://www.parque.ufrj.br/entenda-o-que-sao-e-como-funcionam-as-criptomoedas/. Acesso em: 22 nov. 2023.

RICHARDS, Mark. **Interface Message Processor (IMP)**, 1965. Disponível em: https://www.computerhistory.org/revolution/networking/19/407/2086. Acesso em: 30 out. 2023.

RNP. **Como a Rio-92 possibilitou a primeira rede de internet do país**, 2022. Disponível em: https://www.rnp.br/noticias/como-rio-92-possibilitou-primeira-rede-de-internet-do-pais. Acesso em: 12 jan. 2024.

____. **Evolução do backbone**, 2009a. Disponível em: https://memoria.rnp.br/rnp/backbone-historico.html. Acesso em: 19 nov. 2023.

____. **Linha do Tempo**, 2009b. Disponível em:

https://memoria.rnp.br/rnp/timeline.html. Acesso em: 16 jan. 2024.

____. **Nossa história**, 2023. Disponível em: https://www.rnp.br/sobre/nossa-historia. Acesso em: 16 fev. 2024.

ROCHA, Leonardo. **Exército brasileiro vigia redes sociais para vinda do Papa e Copa do Mundo.** Tecmundo, 2013. Disponível em: https://www.tecmundo.com.br/redes-sociais/42124-exercito-brasileiro-vigia-redes-sociais-para-vinda-do-papa-e-copa-do-mundo.htm. Acesso em: 23 dez. 2023.

RODRIGUES, Luciano Henrique Medeiros. **O amparo jurídico para emprego do exército na segurança pública durante os grandes eventos ocorridos no Rio de Janeiro**, 2018. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/3905/1/MO 6005 - HENRIQUE.pdf. Acesso em: 16 fev. 2024.

RODRIGUES, Roberio Paulino. **O colapso da URSS: um estudo das causas**. Universidade de São Paulo, 2006. Disponível em: https://www.teses.usp.br/teses/disponiveis/8/8137/tde-11072007-112541/publico/TESE_ROBERIO_PAULINO_RODRIGUES.pdf. Acesso em: 16 nov. 2023.

ROHR, Altieres. **Brasil é o país com mais usuários atacados por phishing**. G1, 2019. Disponível em: https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2019/05/20/brasil-e-o-pais-com-mais-usuarios-atacados-por-phishing.ghtml. Acesso em: 27 fev. 2024.

ROHR, Altieres; GOMES, Helton Simões. **Olimpíada Rio 2016 teve quase 3 incidentes cibernéticos por hora**. G1, 2016. Disponível em: https://g1.globo.com/tecnologia/noticia/olimpiada-rio-2016-teve-quase-3-incidentes-ciberneticos-por-hora.ghtml. Acesso em: 20 nov. 2023.

ROMÃO, Wagner de Melo. **As manifestações de junho e os desafios à participação institucional**, 2013. Disponível em: https://repositorio.ipea.gov.br/bitstream/11058/5900/1/BAPI_n04_p11-17_OP_Manifestacoes-junho_Diest_2013-out.pdf. Acesso em: 22 nov. 2023.

ROUSE, Margaret. **What does Cyberspace mean?**, 2023. Disponível em: https://www.techopedia.com/definition/2493/cyberspace#:~:text=Cyberspace refers to

the virtual,used to facilitate online communication. Acesso em: 20 fev. 2024.

RUBIO, Katia. **Dos Jogos Olímpicos que Temos ao Espírito Olímpico que Queremos -** Qual legado Leituras e Reflexões sobre os jogos Olímpicos Rio - 2016, 2018. Disponível em: https://ludopedio.org.br/wp-content/uploads/Jogos_Rio_2016.pdf. Acesso em: 5 dez. 2023.

RÚSSIA, Embaixada da Federação da. **Informação geral**, 2023. Disponível em: https://brazil.mid.ru/pt/r_ssia/informa_o_geral/. Acesso em: 5 out. 2023.

RUSSOBRAS. **Federação da Rússia - Subdivisões da Rússia**, 2023a. Disponível em: https://www.russobras.com.br/subdiv.php. Acesso em: 2 fev. 2024.

_____. **Subdivisões da Rússia - Região Autônoma Judaica**, 2023b. Disponível em: https://www.russobras.com.br/subdiv/judaico.php. Acesso em: 23 dez. 2023.

SÁ, Nelson de. **CDCiber – Centro de Defesa Cibernética inicia em Junho**. **Defesanet**, 2012. Disponível em: https://www.defesanet.com.br/defesa/cdciber-centro-de-defesa-cibernetica-inicia-em-junho/. Acesso em: 19 out. 2023.

SANTOS, Marcos Moreira dos. **Estado, tecnologia e sociedade: a política nacional de informática (Brasil, 1983 - 1984)**. [*s. l.*], 2003. Disponível em: https://repositorio.ufu.br/bitstream/123456789/28579/1/EstadoTecnologiaSociedade.pdf. Acesso em: 22 nov. 2023.

SANTOS, Carlos Pereira dos; PEDRO NETO, João; SILVA, Jorge Nuno. **Livro 4 LEIBNIZ**. Edimpresa, 2007. Disponível em: http://jnsilva.ludicum.org/hm2008_9/Livro4.pdf.

SARAIVA, Márcio. **Um “exame de DNA” na carreira de dois grandes cientistas para descobrirmos o “pai” da nossa profissão**, 2009. Disponível em: http://www.dsc.ufcg.edu.br/~pet/jornal/agosto2009/materias/carreira.html. Acesso em: 19 out. 2023.

SCHIAVI, Iara. **Anonymous cumprem promessa e começam ataques contra Copa do Mundo.** Canaltech, 2014. Disponível em: https://arquivo.canaltech.com.br/hacker/Anonymous-cumprem-promessa-e-comecam-ataques-hackers-contra-Copa-do-Mundo/. Acesso em: 5 out. 2023.

SCHMITT, Michael N. **Tallinn manual on the international law applicable to cyber warfare.** 1ªed. Nova York: Cambridge University Press, 2013.

SEGAL, ADAM. **The Hacked World Order**. 1ªed. New York: Publicafffairs New York, 2016.

SERPRO. **Governo conta com pesquisa e integração para combater ataques cibernéticos**, 2011. Disponível em: https://www.serpro.gov.br/menu/noticias/noticias-antigas/governo-conta-com-pesquisa-e-integracao-para-combater-ataques-ciberneticos. Acesso em: 19 out. 2023.

SHAKARIAN, Paulo. **Análise da Campanha Cibernética da Rússia Contra a Geórgia, em 2008.** Military Review - Revista Profissional do Exército dos EUA - Edição Brasileira, 2011. Disponível em: https://www.armyupress.army.mil/Journals/Edicao-Brasileira/Artigos-em-Destaque/2019/Analise-da-Campanha-Cibernetica-da-Russia-Contra-a-Georgia-em-2008/#:~:text=Especialistas concluíram que hackers georgianos,tenha causado danos significativos22. Acesso em: 15 fev. 2024.

SILVA, Mariana Maria. **Brasil é o 2º país mais vulnerável a ataques de hackers, diz relatório.** Exame, 2023. Disponível em: https://exame.com/future-of-money/brasil-e-o-2o-pais-mais-vulneravel-a-ataques-de-hackers-diz-relatorio/. Acesso em: 14 fev. 2024.

SILVA, João Batista Rodrigues. **Formação continuada de professores que ensinam Matemática: o papel do ábaco na ressignificação da prática pedagógica**. Universidade Federal do Rio Grande do Norte, 2011. Disponível em: https://repositorio.ufrn.br/handle/123456789/16073. Acesso em: 28 dez. 2023.

SIMON, Lmre. **A ARPANET**, 1997a. Disponível em: https://www.ime.usp.br/~is/abc/abc/node20.html. Acesso em: 17 fev. 2024.

_____. **História das Redes no Brasil**, 1997b. Disponível em: https://www.ime.usp.br/~is/abc/abc/node25.html. Acesso em: 18 fev. 2024.

SINGH, Anshuman. **Exploring the Evolution of Generations of Computers**. Shiksha online, 2023. Disponível em: https://www.shiksha.com/online-courses/articles/generation-of-computers/. Acesso em: 19 fev. 2024.

SKLAVENITIS, Dimitris TR. **The Olympic Games of 1896 and 2004 in Athens:**

their undertaking, organisation and impact, 2006. Disponível em: https://www.academia.edu/24298496/The_Olympic_Games_of_1896_and_2004_in_Athens_their_undertaking_organisation_and_impact. Acesso em: 16 fev. 2024.

SOARES, Jussara. **Governo deve apresentar PL para criar agência reguladora de cibersegurança.** CNN Brasil, 2023. Disponível em: https://www.cnnbrasil.com.br/politica/governo-deve-apresentar-pl-para-criar-agencia-reguladora-de-ciberseguranca/#:~:text=O%20governo%20Lula%20deve%20propor,pol%C3%ADtica%20nacional%20sobre%20o%20tema. Acesso em: 01 mar. 2024.

SOARES, Marcelo. **Brazilian Blackout Traced to Sooty Insulators, Not Hackers**. Wired, 2009. Disponível em: https://www.wired.com/2009/11/brazil-blackout/#:~:text=SAO PAULO%2C Brazil — A massive,insulators on two transmission lines. Acesso em: 21 jan. 2024.

SOBREIRA, Vinícius. **Conheça a história das Paralimpíadas, competição nascida num hospital para veteranos de guerra.** Brasil de Fato, 2021. Disponível em: https://www.brasildefatope.com.br/2021/08/19/conheca-a-historia-das-paralimpiadas-competicao-nascida-num-hospital-para-veteranos-de-guerra. Acesso em: 22 nov. 2023.

SOCIETY, Internet. **Donald Davies**. Internet Hall of Fame Pionneer, 2023a. Disponível em: https://www.internethalloffame.org/inductee/donald-davies/. Acesso em: 22 nov. 2023.

_____. **Steve Crocker**. **Internet Hall of Fame Pionneer**, 2023b. Disponível em: https://www.internethalloffame.org/official-biography-steve-crocker/. Acesso em: 25 jan. 2024.

SOUSA, Fernando. **Switch 8 portas: veja sete modelos para comprar no Brasil em 2021**, 2021. Disponível em: https://www.techtudo.com.br/listas/2021/10/switch-8-portas-veja-sete-modelos-para-comprar-no-brasil-em-2021.ghtml. Acesso em: 21 jan. 2024.

SOUZA, Priscilla; GONÇALVES, Andressa. **Tropas militares criam estratégia contra terrorismo em visita do Papa**. G1, 2013. Disponível em: https://g1.globo.com/jornada-mundial-da-juventude/2013/noticia/2013/05/tropas-militares-criam-estrategia-contra-terrorismo-em-visita-do-papa.html. Acesso em: 11

nov. 2023.

SPANIOL, Bruna. **Como o 11/9 mudou a trajetória da proteção de dados**. Aliança, 2015. Disponível em: https://www.aliancatecnologia.com/conteudo/2015/09/como-o-119-mudou-a-protecao-de-dados/. Acesso em: 5 out. 2023.

STEFANO, Fabiane; JANKAVSKI, André; YOSHIDA, Ernesto. **A hora e vez do Governo 4.0**. Revista Exame, 2019. Disponível em: www.exame.com. Acesso em: 22 nov. 2023.

STONE, John. **Cyber War Will Take Place!** Journal of Strategic Studies, v. 36, n. 1, p. 101–108, 2013. Disponível em: https://doi.org/10.1080/01402390.2012.730485. Acesso em: 02 jan. 2024.

STROZI, Guilherme. **Copa das Confederações da Fifa: conheça a história do torneio**. EBC, 2013. Disponível em: https://memoria.ebc.com.br/noticias/esporte/2013/04/copa-das-confederacoes-da-fifa-conheca-a-historia-do-torneio. Acesso em: 24 out. 2023.

SUL21. **Rio+20 terá segurança contra terrorismo e ataques cibernéticos**, 2012. Disponível em: https://sul21.com.br/ultimas-noticias-geral-noticias-2/2012/05/rio-20-tera-grupos-de-seguranca-contra-acoes-terroristas-e-ataques-ciberneticos/. Acesso em: 14 out. 2023.

SUNY, Ronald Grigor. **Ascensão e queda da União Soviética: o império de nações**. Lua Nova: Revista de Cultura e Política, p. 77–98, 2008. Disponível em: https://www.scielo.br/j/ln/a/GRXdNv9DbZzznMGQsrW5sqt/. Acesso em: 11 nov. 2023.

SUNY, Ronald Grigor; DJIBLADZE, Mikhail Leonidovich; LANG, David Marshall. **Georgia**, 2023. Disponível em: https://www.britannica.com/place/Georgia/People. Acesso em: 18 nov. 2023.

TEIXEIRA, Carlos Alberto. **Vírus Stuxnet, que atacou usinas nucleares no Irã, foi criado em parceria por EUA e Israel**. O Globo Economia, 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: 22 nov. 2023.

TONOOKA, Eduardo Kiyoshi. **Política nacional de informática: vinte anos de**

intervenção governamental. Estudos Econômicos, v. 22, n. 2, p. 273–297, 1992. Disponível em: https://www.revistas.usp.br/ee/article/view/158841/153819. Acesso em: 22 nov. 2023.

TRUJILLO, Clorinda. **The Limits of Cyberspace Deterrence**, p. 43–52, 2014. Disponível em: https://apps.dtic.mil/sti/citations/tr/ADA622249. Acesso em: 26 out. 2023.

UEM, Universidade Estadual de Maringá -. **História dos Computadores no Brasil**. Maringá - PR, 1996. Disponível em: http://ws2.din.uem.br/~museu/hist_nobrasil.htm. Acesso em: 16 fev. 2024.

UFMG. **Como estão as antigas repúblicas que integravam a União Soviética?**, 2017. Disponível em: https://ufmg.br/comunicacao/noticias/como-estao-as-antigas-republicas-que-integravam-a-uniao-sovietica. Acesso em: 22 nov. 2023.

US-CCU. **Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008.** A US-CCU Special Report, 2009. Disponível em: https://indianstrategicknowledgeonline.com/web/US-CCU-Georgia-Cyber-Campaign-Overview.pdf. Acesso em: 22 nov. 2023.

USP. **Projeto a respeito de uma nova enciclopédia que deve ser redigida pelo método da descoberta**. Scientia Agricola, v. 5, n. 1, 2007. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1678-31662007000100006&lng=pt&nrm=iso&tlng=pt. Acesso em: 27 fev. 2024.

VALLE, Sabrina. **Fontes da CIA afirmam que ataques de hackers já provocaram ao menos dois apagões no Brasil**. O Globo Economia, 2009. Disponível em: https://oglobo.globo.com/economia/fontes-da-cia-afirmam-que-ataques-de-hackers-ja-provocaram-ao-menos-dois-apagoes-no-brasil-3159097. Acesso em: 15 fev. 2024.

VAN VUUREN, Jj *et al.* **Building blocks for national cyberpower**, 2016. Disponível em: https://researchspace.csir.co.za/dspace/bitstream/handle/10204/8867/Van Vuuren_2016.pdf?sequence=1&isAllowed=y. Acesso em: 24 out. 2023.

VEGH, Sandor. **Classifying forms of online activism: the case of cyberprotests against the World Bank**. *In*: MCCAUGHEY, Martha; AYERS, Michael D. (org.). Cyberactivism: online activism in theory and practice. Nova York e Londres: Routledge, 2003.

VENTRE, Daniel. **Seguridad global y Potencias emergentes en mundo multipolar**. *In*: , 2012. Ciberguerra, 2012. Disponível em: https://publicaciones.defensa.gob.es/media/downloadable/files/links/P/D/PDF48.pdf. Acesso em: 27 jan. 2024.

VIANA, Alexander Martins. **Russificação Soviética e Pós-soviética: Autoridade Política e Etnicidade, 1917-1997**. Rio de Janeiro, RJ, 2019. Disponível em: https://periodicos.uff.br/cantareira/article/view/27771. Acesso em: 15 fev. 2024.

VIEIRA, Eduardo. **Os bastidores da Internet no Brasil**. Manole Ltda, 2003.

WASHINGTON. **Snowden diz que recebeu treino de espião**. Agência Brasil - EBC, 2014. Disponível em: https://agenciabrasil.ebc.com.br/internacional/noticia/2014-05/snowden-diz-que-recebeu-treino-de-espiao. Acesso em: 23 dez. 2023.

WHITMORE, Brian. **Is The Clock Ticking For Saakashvili?** Radio Free Europe/Radio Liberty, 2008. Disponível em: https://www.rferl.org/a/Is_The_Clock_Ticking_For_Saakashvili/1199512.html. Acesso em: 2 fev. 2024.

WHYTE, Andrew. **Russian authorities to install tank monument across river from Narva**, 2022. Disponível em: https://news.err.ee/1608701224/russian-authorities-to-install-tank-monument-across-river-from-narva. Acesso em: 19 fev. 2024.

WIKILEAKS. **Brazil: Blackout – Causes and implications**. WIKILEAKS - Public Library of US Diplomacy, 2009. Disponível em: https://wikileaks.org/plusd/cables/09BRASILIA1382_a.html. Acesso em: 9 mar. 2024.

YIN, Robert K. **ESTUDO DE CASO: Planejamento e Métodos**. 2. ed. Porto Alegre: Bookman, 2001.

YOUNG, David C. **A Brief History of the Olympic Games**. Malden - MA - USA: Blackwell Publishing, 2004.

YOUNG, David; ABRAHAMS, Harold Maurice. **Olympic Games**, 2024. Disponível em: https://www.britannica.com/sports/Olympic-Games. Acesso em: 16 fev. 2024.

ZETTER, Kim. **Countdown to Zero Day : Stuxnet and the launch of the world's first digital weapon**. New York: Crown Publishers, 2014.

_____. **How digital detectives deciphered Stuxnet, the most menacing malware in history**. Wired.com, 2011. Disponível em: https://arstechnica.com/tech-policy/2011/07/how-digital-detectives-deciphered-stuxnet-the-most-menacing-malware-in-history/. Acesso em: 21 jan. 2024.

Apêndice A - Principais eventos cronológicos da Informática brasileira

Principais eventos cronológicos da Informática brasileira	
1917	A IBM inicia suas operações no Brasil. Através de um contrato de prestação de serviços, surge no Brasil a empresa norte americana *Computing Tabulating Recording Company*, que em 1924, sob a liderança de Thomas J. Watson, foi registrada nos Estados Unidos como *International Business Machines Corporation* (IBM).
1924	A IBM é autorizada a operar no Brasil por um decreto assinado pelo presidente Arthur Bernardes.
1939	Inaugurada no Brasil a primeira fábrica da IBM fora dos Estados Unidos, localizada no bairro de Benfica, no Rio de Janeiro.
1957	Chegou um Univac-120, o primeiro computador no Brasil, adquirido pelo Governo do Estado de São Paulo, era usado para calcular todo o consumo de água na capital. Ocupava o andar inteiro do prédio onde foi instalado. Equipado com 4.500 válvulas, fazia 12 mil somas ou subtrações por minuto e 2.400 multiplicações ou divisões, no mesmo tempo.
1959	A empresa Anderson Clayton compra um Ramac 305 da IBM, o primeiro computador do setor privado brasileiro. Dois metros de largura, um metro e oitenta de altura, ocupava um andar inteiro da empresa. A empresa foi uma das primeiras fora dos Estados Unidos a usar esse computador.
1961	- (Zezinho) - Como trabalho de fim de curso de engenharia eletrônica no ITA e auxílio financeiro do CNPq de 350 dólares, quatro alunos, José Ellis Ripper, Fernando Vieira de Souza, Alfred Wolkmer e Andras Vásárhelyi auxiliados pelo chefe da Divisão de Eletrônica do ITA e professor Richard Wallauschek construíram o "Zezinho". Com os recursos disponíveis não foi possível construir um computador com grande capacidade de memória, o painel tinha dois metros de largura por um metro e meio de altura, foram utilizados cerca de 1500 transistores e diodos de fabricação nacional, produzidos pela Ibrape, uma subsidiária da Philips, tinha capacidade para fazer vinte operações. Era um computador didático, para uso em laboratório. Ganhou, entretanto, lugar na história como o primeiro computador não-comercial transistorizado totalmente nacional projetado e construído no Brasil, embora um sucesso, foi desmontado

	pelos alunos das turmas seguintes, que utilizaram seus circuitos para novas experiências. - A Fábrica da IBM, em Benfica-RJ, inicia a montagem de computadores da linha 1401.
1964	01/dezembro - Criado o Serpro - Serviço Federal de Processamento de Dados, empresa pública criada para modernizar e dar agilidade a setores estratégicos da administração pública.
1968	1º Congresso Nacional de Informática - CNI.
1969	24/julho - Criada a Prodesp - Companhia de Processamento de Dados do Estado de São Paulo.
1971	Entra em operação a fábrica da IBM na cidade de Sumaré/SP.
1972	- 05/abril - Criado a CAPRE - Comissão de Coordenação das Atividades de Processamento Eletrônico, órgão governamental cujo objetivo inicial era promover o uso mais eficiente dos computadores na administração pública e traçar uma política tecnológica para a área de informática. - julho - Construído o "Patinho Feio" no Laboratório de Sistemas Digitais - LSD da Escola Politécnica da USP, foi concebido como um trabalho de fim de curso. O Patinho Feio é tido como o primeiro computador, documentado e com estrutura de computação clássica, desenvolvido no Brasil. Tinha um metro de comprimento, um metro de altura, 80 centímetros de largura, pesava mais de 100 quilos e possuía 450 pastilhas de circuitos integrados, formando 3 mil blocos lógicos distribuídos em 45 placas de circuito impresso. A memória podia armazenar 4.096 palavras de 8 bits, ou seja, 4K. O Patinho feio se tornou um marco inicial porque gerou massa crítica para a consolidação da indústria de informática no Brasil.
1974	18/julho - Fundação da COBRA - Computadores e Sistemas Brasileiros Ltda. A Cobra foi a primeira empresa brasileira a desenvolver, fabricar e comercializar computadores.
1975	- Fundação do LSI - Laboratório de Sistemas Integráveis na Escola Politécnica da USP. - junho - Fundação da Scopus, uma das principais empresas de informática do Brasil. Empresa criada por um grupo de ex-professores da Poli-USP que trabalharam no desenvolvimento do minicomputador G-10.

	- agosto - Lançamento da revista Dados & Idéias. Revista lançada pelo Serpro para mostrar a realidade tecnológica no Brasil. Periodicidade bimestral.
1976	- janeiro - Fundada a SID - Sistemas de Informação Distribuída S/A. - julho - Fundada em Porto Alegre a SBC - Sociedade Brasileira de Computação. A SBC é uma instituição acadêmica que incentiva e desenvolve pesquisa científica na área da computação no Brasil.
1979	- 09/outubro - Criado a SEI - Secretaria Especial de Informática. Após ampla reestruturação dos órgãos governamentais responsáveis pelo setor de informática, a Capre foi substituída pela SEI na formulação da Política Nacional de Informática. - Fundada a Elebra Informática S/A, grande fabricante de impressoras, entre elas a matricial Emília.
1980	- Pela primeira vez um microcomputador era vendido em um grande magazine. Entre vitrinas com eletrodomésticos, ofertas de cama, mesa e banho, miudezas, câmaras fotográficas e calculadoras, o Mappin da Praça Ramos, no centro de São Paulo, vendia o D-8000, microcomputador da Dismac. - Lançado pela Cobra na SUCESU de 1980 o primeiro minicomputador totalmente projetado, desenvolvido e fabricado no Brasil a alcançar o mercado, o Cobra 530.
1981	- Fundação da Microdigital, foi na primeira metade da década de 80 o maior fabricante nacional de microcomputadores. Famosa pelos seus micros da linha Sinclair como o TK-85, TK-90X e TK-95. - Desenvolvido o Sistema 700 da Prológica, microcomputador de uso profissional de 8 bits. - outubro - Lançamento da revista MicroSistemas, primeira publicação brasileira dedicada exclusivamente aos microcomputadores. - 16 - 23/outubro - Realizada a I Feira Internacional de Informática no Pavilhão de Exposições do Parque Anhembi/SP, teve 117.253 visitantes e 183 expositores. Foi um evento paralelo à realização do XIV CNI - Congresso Nacional de Informática. - 23/outubro - Inaugurado o 1º laboratório de microinformática no Brasil, instalado numa sala dentro da biblioteca da Faculdade de Economia e

	Administração da USP, tinha cinco microcomputadores D-8000, cedidos pela Dismac. O laboratório era aberto a todos os alunos da universidade.
1982	Fevereiro - Fundado o IBPI - Instituto Brasileiro de Pesquisa em Informática, instituto criado para o ensino de profissionais de informática, no Rio de Janeiro/RJ.
1983	Março - Lançado o microcomputador EGO pela empresa Softec, primeiro microcomputador brasileiro a utilizar a tecnologia dos microprocessadores de 16 bits, compatível com o IBM PC, era baseado no microprocessador 8080 da Intel e clock de 5 MHz.
1984	- Lançado pela Telesp - Companhia Telefônica do Estado de São Paulo o primeiro sistema de videotexto brasileiro. O teste piloto ocorreu de 1982 a 1984 com 1.500 assinantes da Telesp. - 29/outubro - Sancionada a Lei nº 7.232 que estabelecia os princípios, objetivos e diretrizes da Política Nacional de Informática, estava criada a reserva de mercado de informática no Brasil.
1985	Agosto - Fundada a Gradiente Informática, fabricante do Expert, microcomputador de 8 bits da linha MSX.
1986	09/setembro - Fundada em São Paulo a ABES - Associação Brasileira das Empresas de Software.
1987	- Criação da Fácil Informática, empresa desenvolvedora do editor de textos Fácil. - 24 - 27/março - 1º FENASOFT - Feira Nacional do Software, no Riocentro, Rio de Janeiro.
1995	- 26 - 29/setembro - Realizado a COMNET Fenasoft Brazil´95 no Pq. Anhembi em São Paulo, evento internacional de telecomunicações e redes. - Realizado o I CONIP - Congresso Nacional de Informática Pública, em São Paulo. Fórum para discussão e apresentação do uso da tecnologia da informação no serviço público.

Fonte: (UEM, 1996)

Apêndice B – Antecedentes e Cronologia do Stuxnet

Data	Evento
29/01/2002	George Bush faz seu famoso discurso sobre o estado da união ao Congresso dos EUA descrevendo a Coreia do Norte, o Irã e o Iraque como um "eixo do mal" para tentar desenvolver armas de destruição em massa. Com efeito, Bush prometeu desarmá-los, quer por meios militares ou outros, e fazê-lo mais cedo ou mais tarde (ECONOMIST, 2002).
08/2002	Um grupo dissidente iraniano revela que seu governo está enriquecendo urânio na sua instalação nuclear em Natanz. Os EUA reagem afirmando que o Irã está tentando desenvolver armas nucleares.
02/2003	O Irã revela que está enriquecendo urânio em Natanz. Subsequentemente, os inspetores da Agência Internacional de Energia Atômica (AIEA) programam uma primeira visita a planta nuclear e posteriores visitas a instalação de forma a serem realizadas regularmente.
2006	O Conselho de Segurança da ONU adota por unanimidade a Resolução 1737, impondo sanções ao Irã por não ter suspendido as suas atividades relacionadas com o enriquecimento do urânio. As sanções proíbem os países de transferirem tecnologia sensível relacionada às armas nucleares e aos mísseis para o Irã e exigem que todos os países congelem os ativos de dez organizações iranianas e de doze indivíduos pelo seu envolvimento nos programas nuclear e de mísseis do Irã (DAVENPORT, 2023).
06/2010	VirusBlockAda, uma empresa de antivírus baseado na Bielorrússia, descobre o Stuxnet worm depois que a empresa recebe uma amostra do malware que estava causando o reinício contínuo de um computador da Usina de Natanz. Esse software malicioso surpreendeu os especialistas por ser malware de exploração dia zero o que era incomum para um *worm* de computador (ZETTER, 2011).
12/07/2010	A notícia da descoberta de um worm de computador usando um malware de dia zero tornou-se público e o antivírus e as comunidades tecnológicas começaram a fazer uma engenharia reversa e a investigar esse malware. Neste momento, acreditava que o Stuxnet era uma ferramenta para

	espionagem industrial. Sua sofisticação sugere que recursos financeiros significativos foram investidos em seu desenvolvimento (ZETTER, 2011).
08/2010	A empresa de antivírus Symantec revela que o propósito do *worm* é sabotagem e não espionagem (ZETTER, 2011), na verdade, os especialistas reconstituem a origem do *worm* em cinco organizações no Irã, confirmando que o país foi o ponto de partida e provavelmente também o alvo das infecções (LINDSAY, 2013, p. 380 *apud* BAEZNER; ROBIN, 2017). No mesmo período, verifica-se que os servidores do Comando e Controle do Stuxnet (C&C) perderam conexão com os computadores infectados no Irã. Especialistas acreditam que esta desconexão significa que o Irã estava tentando lidar com o verme para conter sua propagação (ZETTER, 2011b *apud* BAEZNER; ROBIN, 2017). A usina elétrica de Bushehr, no Irã deveria lançar sua unidade de energia nuclear, mas atrasou o lançamento. Fontes oficiais do Irã informaram que o atraso se deu em razão de problemas técnicos não especificados (COLLINS; MCCOMBIE, 2012, p. 85).
09/2010	Autoridades iranianas admitem que alguns computadores pessoais de funcionários da a usina nuclear de Bushehr está infectada por um vírus de computador. Eles acusam países ocidentais de estarem por trás do ataque (FARWELL; RAFAL ROHOZINSKI, 2011, p.25).
11/2010	O Irã interrompe o seu enriquecimento de urânio na Usina Nuclear de Natanz sem apresentar qualquer motivo (FARWELL; Rafal ROHOZINSKI, 2011). Mais tarde confirmou que esta foi uma tentativa de eliminar o Stuxnet da usina. O líder da Organização de Energia Atómica do Irã e o Ministro das Relações Exteriores em exercício na época, admitiram que um malware de computador infectou as instalações nucleares iranianas (ALBRIGHT; BRANNAN; WALROND, 2010, p. 02).
12/2010	O Instituto de Ciência e Segurança Internacional (ISIS), uma instituição sem fins lucrativos sediada nos EUA que monitora a evolução do programa nuclear do Irã desde a década de 1990, confirma que o worm

	Stuxnet é programado para atingir elementos configurado da mesma maneira que o centrífugas Natanz.

Fonte: (BAEZNER; ROBIN, 2017, p.6-7)